

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

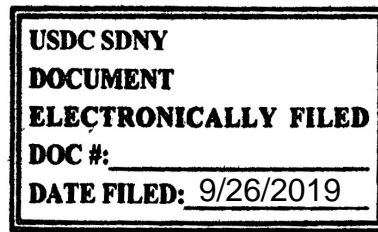
JOINT STOCK COMPANY CHANNEL ONE
RUSSIA WORLDWIDE, et al.,

Plaintiffs,

-against-

INFOMIR LLC, et al.,

Defendants.



16-CV-1318 (GBD) (BCM)

OPINION AND ORDER

BARBARA MOSES, United States Magistrate Judge.

By motion dated November 5, 2018 (Dkt. No. 692), defendant Infomir LLC (Infomir) seeks discovery sanctions against plaintiffs for their repeated failure to produce electronically stored information (ESI) evidencing an investigation conducted in May 2016 by Christopher Vidulich, a paralegal employed by plaintiff's counsel, who used the "Wireshark" network protocol analyzer in an effort to determine the source of a video stream that he viewed through an Infomir brand internet protocol television (IPTV) receiver (the Wireshark Investigation). Vidulich first described his investigation in an affidavit dated June 24, 2016 (the Vidulich Affidavit), which plaintiffs filed in support of their successful motion for leave to amend their initial Complaint. Since then, plaintiffs have continued to rely on the Vidulich Affidavit – refiling it verbatim as an exhibit to their First Amended Complaint (FAC) and referencing it repeatedly in other filings – in support of their contention that Infomir unlawfully "streams" an unauthorized version of plaintiffs' television programming to consumers in the United States over the internet.

The only complete record of the Wireshark Investigation is a native-format electronic "packet capture" file that Vidulich saved to the laptop computer on which he conducted the investigation (the Firm Laptop) under the name "Channel One Capture.pcapng" (the Channel One PCAP). However, plaintiffs did not produce the Channel One PCAP to Infomir for more than two years, until October 12, 2018. They failed to produce it as part of their automatic disclosures

pursuant to Fed. R. Civ. P. 26(a)(1)(A); failed to produce it in response to Infomir's May 3, 2017 request for all documents "relating to any inspection, test or examination of any device alleged to be originating from or the responsibility of Infomir"; failed to produce it in response to an April 12, 2018 subpoena *duces tecum* addressed to Vidulich himself, seeking "all documentation related to, and data collected from" the Wireshark Investigation; failed to produce it in response to this Court's Discovery Order dated April 25, 2018, instructing plaintiffs to turn over "any additional documents in their possession, custody, or control . . . constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities"; and failed once again to produce it in response to this Court's Order dated July 3, 2018, directing them to "conduct a further search of their records, including ESI, and [] produce any additional documents constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities."

On or about June 22, 2018 – while subject to, and purportedly in furtherance of, the April 25, 2018 Discovery Order – Vidulich moved the Channel One PCAP from the Firm Laptop to another computer at the offices of plaintiffs' counsel. Consequently, on July 2, 2018, when plaintiffs turned over the Firm Laptop for imaging and inspection by Infomir's experts, the Channel One PCAP was no longer on it. On August 29, 2018, Vidulich testified under oath that the Wireshark data underlying the Vidulich Affidavit "wasn't saved." That was not true. However, under increasing pressure from Infomir – which on September 14, 2018, requested leave to move for spoliation sanctions – Vidulich reaffirmed his untruthful testimony in a sworn affidavit dated September 21, 2018, once again stating, under oath, that he did not save any data from the investigation described in his original affidavit, except in the form of screenshots, and that plaintiffs had already produced "everything that was retained." As late as October 5, 2018 – after

Infomir's forensic experts discovered (and explained to plaintiffs) that there had once been a native-format Wireshark file called "Channel One Capture.pcapng" on the Firm Laptop, but that it was no longer there – plaintiffs' counsel again denied that any such file existed, and insisted that they had turned over "[e]verything that was saved."

On October 12, 2018, when plaintiffs' lawyers finally produced the Channel One PCAP, they explained that its earlier "omission" was "inadvertent" – relying on another affidavit from Vidulich in which he stressed his lack of "specialized technical knowledge" – and blamed Infomir for the delay, on the theory that it should have forensically examined the Firm Laptop earlier than it did. Plaintiffs did not disclose (and would not, for another two months) that Vidulich was taught how to use the Wireshark program and analyze its results by Dmitri Dietrich, the Chief Technology Officer of Kartina Digital GmbH (Kartina). Although not formally a party to this action, Kartina pays plaintiffs' legal fees and coordinates their legal strategy.

After producing the Channel One PCAP, plaintiffs demanded that Infomir withdraw its September 14, 2018 request because "there was no spoliation vis-à-vis the '.pcap' file as wrongfully alleged." Infomir agreed that the issue was no longer "one of spoliation," and instead moved for sanctions pursuant to Fed. R. Civ. P. 37(b) and this Court's inherent powers, arguing that plaintiffs and their counsel violated multiple discovery orders, made a series of false statements to the Court, and engaged in related obstructive tactics designed to prevent Infomir from discovering that the Channel One PCAP "fundamentally contradicts" Vidulich's sworn description of the May 2016 Wireshark Investigation and its results.

In support of its motion, Infomir has presented credible expert evidence demonstrating that the Wireshark Investigation did not occur on the date or in the manner repeatedly sworn to by

Vidulich. These facts have been largely corroborated by plaintiffs' expert – the same Dmitri Dietrich who taught Vidulich how to use Wireshark – and are now conceded by Vidulich himself. Moreover, both sides' experts agree that the key factual assertion in the Vidulich Affidavit – that he “trace[d] the source” of an unauthorized IPTV stream of one of plaintiffs' channels to a specific domain, “freetvstat.iptv.infomir.com.ua,” affiliated with Infomir, with an IP address located in the United States – was inaccurate. The long-withheld Channel One PCAP shows that “freetvstat.iptv.infomir.com.ua” was not the source of the unauthorized video stream.

For the reasons set forth below, Infomir's motion will be granted. As a sanction, the Court will preclude plaintiffs from introducing or relying on the Vidulich Affidavit, any other report of, testimony about, or opinions based on the Wireshark Investigation, and any data or information captured during that Wireshark Investigation, including but not limited to the Channel One PCAP. In addition, plaintiffs and their counsel must reimburse Infomir for its attorney's fees, expert fees, and other costs reasonably incurred in uncovering the Channel One PCAP and making its sanctions motion.

I. BACKGROUND

Plaintiffs Joint Stock Company Channel One Russia Worldwide (Joint Stock Company Channel One), Closed Joint Stock Company CTC Network, Closed Joint Stock Company TV DARIAL, Closed Joint Stock Company “New Channel,” Limited Liability Company “Rain TV-Channel,” and Limited Liability Company “Comedy TV,” n/k/a Limited Liability Company Global Entertainment TV, are a group of Russian television broadcasters (sometimes referred to as the Broadcasters), suing to redress what they characterize as the “pirating” and resale of their television programming to consumers in the United States, over the internet, without authorization

or license fees. *See* FAC (Dkt. No. 211) ¶ 1. Plaintiffs are “organized under the laws of the Russian Federation,” *id.* ¶¶ 6, 15, 19, 21, 23, 26, and most are headquartered in Moscow. *Id.* ¶¶ 6, 23, 26. Their programming is broadcast via satellite in Russia and neighboring countries. *Id.* ¶ 62. Defendant Infomir is a New York limited liability company. *Id.* ¶ 30 & Ex. 5.¹

A. The Original Complaint

Plaintiffs filed this lawsuit on February 19, 2016, against nine different defendants, charging generally that all of them engaged in the “unauthorized interception, copying and distribution of encrypted transmissions of [the] Broadcasters’ famous Channels and Programming to paying consumers in this judicial district and throughout the United States,” in violation of, *inter alia*, § 605(a) of the Federal Communications Act (FCA), 42 U.S.C. § 605(a); the Copyright Act, as amended by the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201 *et seq.*; § 43 of the Lanham Act, 15 U.S.C. § 1125; and § 349 of the New York General Business Law (GBL). Compl. (Dkt. No. 1) ¶¶ 6, 92-156. According to plaintiffs, all defendants “hack, capture or otherwise acquire without permission the encrypted signals of the Plaintiffs’ Channels and transmit those signals to its servers which in turn stream the wrongfully acquired signals over IPTV to paying customers in this judicial district and elsewhere.” *Id.* ¶ 86.

¹ The factual background and procedural history of this action, as relevant to the instant sanctions motion, are described in more detail in the Court’s prior opinions in this action, including *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2017 WL 696126 (S.D.N.Y. Feb. 15, 2017), *report and recommendation adopted*, 2017 WL 2988249 (S.D.N.Y. Mar. 27, 2017); *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2018 WL 2932725 (S.D.N.Y. June 12, 2018); *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2018 WL 4681616 (S.D.N.Y. Sept. 11, 2018), *report and recommendation adopted*, 2018 WL 4666069 (S.D.N.Y. Sept. 28, 2018); *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2018 WL 4907911 (S.D.N.Y. Sept. 25, 2018); *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2018 WL 6712769 (S.D.N.Y. Nov. 30, 2018). Familiarity with these opinions is assumed.

As to some of the defendants, plaintiffs provided supporting facts or exhibits. *See, e.g.*, Compl. ¶ 87 & Ex. 11 (alleging that defendant Actava TV, Inc. streamed plaintiff's channels through its website www.actava.tv). As to Infomir, however, plaintiffs' only specific factual allegations were that it maintained an interactive website, *id.* ¶¶ 7, 55, through which it was "selling receivers with which it is possible to receive Plaintiffs' channels without authorization." *Id.* ¶ 56; *see also id.* ¶ 90(b) & Ex. 14 (showing "Infomir's homepage offering receiver boxes").

B. Kartina

The Broadcasters are not the only entities with an interest in policing unauthorized transmission of their content. Plaintiffs distribute their programming through various licensees, including Kartina, which offers plaintiffs' Russian-language channels to U.S. consumers over IPTV for a monthly subscription fee of \$29 (in 2018). *See* Panfilova Decl. (Dkt. No. 629) ¶¶ 3, 8, 31. Kartina suffers economically when "pirates" offer the same or similar subscription services at cut-rate prices. *See id.* ¶ 5 ("many pirates in the U.S." charge "50% to 70% less than Kartina does for Broadcasters' content because Kartina pays substantial license fees for Broadcasters' content."); *id.* ¶¶ 28-31 (listing 11 "major pirates" and comparing their prices to Kartina's).

Although Kartina is not named as a plaintiff in this action, it is Kartina – not the Broadcasters – that retained the law firm Dunnington, Bartholew & Miller LLP (Dunnington), which now serves as plaintiffs' counsel of record, to investigate and prosecute this and other "piracy" actions. Panfilova Decl. ¶¶ 7-8 & Exs. B, C. Similarly, it is Kartina – not the Broadcasters – that pays Dunnington's fees. *Id.* Prior to the disclosure of these facts in 2018, Kartina's role was kept confidential, for "commercial reasons." *Id.* ¶ 15. Kartina works "very closely with Dunnington," "crafting pleadings and coordinating a joint legal strategy to be pursued on behalf

of the Broadcasters.” *Id.* ¶ 17. Kartina claims that it, like plaintiffs themselves, has an attorney-client relationship with Dunnington, and has repeatedly invoked the attorney-client privilege and/or the work product doctrine to shield its communications with Dunnington and some of its investigatory activities. *See, e.g., id.* ¶¶ 17-19.

C. Infomir’s Motion to Dismiss

On June 2, 2016, Infomir moved to dismiss the claims against it pursuant to Fed. R. Civ. P. 12(b)(6), arguing that it was differently situated from its co-defendants:

Regarding Infomir, the complaint alleges only that Infomir manufactures and sells set-top IPTV receivers which can be purchased from Infomir’s website on the world-wide-web and which are capable of receiving IPTV streams over the internet. It does not allege that Infomir’s IPTV set top boxes are illegal nor that their use is intended for or limited to nefarious purposes. Rather, the complaint alleges simply that with an Infomir set top box, “it is possible to receive Plaintiffs’ channels without authorization.” ¶ 56. These are the only facts pleaded against Infomir. Accepted as true, they are insufficient to support a finding of liability against Infomir.

Infomir Mem. dated June 2, 2016 (Dkt. No. 67), at 1; *see also id.* at 5 (“Plaintiffs do not allege that Infomir is involved in obtaining, decrypting or broadcasting their content.”). Therefore, Infomir argued, plaintiffs failed to state any claim against it under the FCA, the Lanham Act, the Copyright Act, or the GBL. *Id.* at 9-20.

D. The Vidulich Affidavit

Plaintiffs opposed the motion to dismiss and cross-moved for leave to amend, relying in substantial part on the June 24, 2016 Vidulich Affidavit. *See* Notice of Cross-Motion (Dkt. No. 78) at 1; Vidulich Aff. (Dkt. No. 80) ¶ 1.² Vidulich was employed by Dunnington as a paralegal.

² Vidulich has submitted multiple affidavits over the course of this action. Unless otherwise specified, references in this Opinion and Order to the “Vidulich Affidavit” or “Vidulich Aff.” are

Vidulich Aff. ¶ 1. The purpose of his affidavit was to “explain the functionality” of Infomir’s set-top boxes (STBs), “using the example of Infomir’s AURA HD box.” *Id.* ¶ 2. Carefully noting that he had no “specialized technical knowledge,” *id.* ¶ 3, Vidulich explained (relying in part on a Wikipedia article) that the AURA HD is a “specialized type” of STB, called an “IPTV receiver,” that can (among other things) receive, decode, and play “video streaming media” delivered over the internet. *Id.* ¶ 9 & Ex. 3. The AURA HD that Vidulich obtained for purposes of his affidavit was apparently manufactured by Telecommunication Technologies, Ltd. (Teletec), a Ukrainian entity which is allegedly affiliated with Infomir, *see* FAC ¶ 32, but is not a party to this action. Vidulich Aff. ¶ 11 & Ex. 5.

Vidulich attested that on May 13, 2016, he connected the AURA HD box to a projector and a laptop computer, logged onto Dunnington’s wireless internet connection, and was able to watch Russian-language programming, including Channel One (a channel produced by lead plaintiff Joint Stock Company Channel One). Vidulich Aff. ¶¶ 11-17 & Exs. 6-13. It is not clear from the Vidulich Affidavit whether, as part of the experiment, Vidulich also logged into a third-party IPTV subscription service.³

Vidulich further attested that on May 27, 2016, he set out to “analyze the source of the content being streamed into the AURA HD box.” Vidulich Aff. ¶ 19. He used Wireshark, a “network protocol analyzer” that could “capture the Internet Protocol [IP] addresses of the sources

to his affidavit dated June 24, 2016, first filed at Dkt. No. 80. References to affidavits signed by Vidulich on other dates are cited as “[date] Vidulich Aff.”

³ There are many such services available in the marketplace. As noted above, Kartina offers plaintiffs’ programming to U.S. consumers over IPTV for a monthly subscription fee. *See* Panfilova Decl. ¶¶ 3, 8, 31. In addition, plaintiffs allege that there are many “pirate” entities offering similar services at cut-rate prices. *See* FAC ¶¶ 4, 37-38; Panfilova Decl. ¶¶ 5, 28-31.

sending video streaming media” to the STB while he was using it to view Channel One. *Id.* ¶¶ 20-23. According to his affidavit, Vidulich “scanned through the activity that was captured while the Channel One Stream was active,” and saw that “the AURA HD box connected to ‘freetvstat.iptv.infomir.com.ua,’” at the IP address 66.234.224.2, *id.* ¶ 24, and later that it connected to a “stalker portal,” at the IP address 37.58.59.33, which he believed to be a reference to the “Stalker Middleware” offered by Infomir. *Id.* ¶ 26. Vidulich attached two screenshots (the Channel One Screenshots) of what he called Wireshark “readouts” displaying the STB’s “connection with Infomir.” *Id.* ¶¶ 24, 26, Exs. 14, 16. At the bottom of each Channel One Screenshot is the date – May 27, 2016 – and in the top left-hand corner is the name of the file that was open when the screenshot was taken: “Channel One Capture.pcapng.” *Id.* Exs. 14, 16.⁴

Vidulich consulted another website, “www.iplocation.net,” from which he learned that the IP address 66.234.224.2 was located “within the United States.” Vidulich Aff. ¶ 25 & Ex. 15.

Vidulich noted that Infomir claimed, on its own website, that it is “not involved in any content distribution activity.” Vidulich Aff. ¶ 30. However, he concluded, “this assertion appears to be incorrect in light of the fact that *I was able to trace the source of Channel One to freetvstat.iptv.infomir.com.ua.*” *Id.* ¶ 30 (emphasis added).

⁴ The first Channel One Screenshot (originally attached as Exhibit 14 to the Vidulich Affidavit) is reproduced the Appendix to this Opinion and Order. It shows a multi-column table that lists, among other things, the “source” and “destination” of the data being transmitted in each “packet” that was captured by the Wireshark program. Approximately one-third of the way down the table, at packet No. 72 (with the time stamp 22.970968), the screenshot appears to show that Vidulich’s STB was communicating with a “destination” server at the IP address 66.234.224.2. In the corresponding “info” column, the screenshot displays: “Standard query 0x1c60 A freetvstat.iptv.infomir.com.ua.” At packet 73 (with the timestamp 22.980869), the screenshot appears to show that the STB was receiving a communication from a “source” server at the same IP address. The “info” column reads, “Standard query response 0x1c60 Refused A freetvstat.iptv.infomir.com.ua.” These lines are highlighted the Appendix.

E. Wireshark

Plaintiffs and Infomir have provided the Court with expert declarations and testimony explaining what Wireshark is and how it captures and stores information. Infomir submitted a report by Christopher T. Rucinski,⁵ who explains:

Wireshark . . . is a software program that allows a user to create a record of data packets transmitted across a computer network by “capturing” the data packets in a file. Wireshark can also be utilized by a user to subsequently analyze the captured data packets, and such analysis can include identifying the source, destination, and content of the captured data packets. The file format in which Wireshark captures data packets is sometimes referred to as “PCAP” format, which is short for “Packet Capture,” and such files typically have a file extension of “.pcap.”

Rucinski Rep. at 1-2.

Plaintiffs submitted the Declaration of Dmitri Dietrich,⁶ who agrees that “Wireshark is a software program that allows a user to record data transmission across computer networks by capturing data in a file. The file format in which Wireshark stores captured data is the ‘PCAP’ format with file extension ‘.pcap’ or ‘.pcapng.’” Dietrich Decl. ¶ 7. Thus, as Dietrich confirms, “[t]he Channel One PCAP” that was open on Vidulich’s laptop when he took the Channel One Screenshots was “saved with the file extension ‘.pcapng’ indicating that the file is a PCAP file and can therefore be opened and analyzed on Wireshark.” *Id.*

⁵ Rucinski holds an A.B. in computer science from Princeton University and has worked since 2010 as a consultant, first at Elysium Digital LLC (Elysium), and then at Stroz Friedberg LLC (Stroz Friedberg), which acquired Elysium in 2015. *See* Rucinski Rep. (Dkt. No. 694-1) at 1.

⁶ Dietrich holds a degree in computer science from Fachhochschule Wiesbaden (now known, in English, as the RheinMain University of Applied Sciences). Dietrich Decl. (Dkt. No. 708) ¶ 4. As of the date of his declaration, he had worked for Kartina for nearly 12 years and served as its Chief Technical Officer in Weisbaden, Germany. *Id.* ¶¶ 1, 3.

F. Plaintiffs' Cross-Motion to Amend

Plaintiffs opposed Infomir's motion to dismiss the claims against it and cross-moved for leave to amend. In their accompanying brief, they relied heavily on the conclusions drawn by Vidulich from his Wireshark Investigation, asserting – among other things – that the “Channel One stream accessible by [Infomir's] AURA HD set-top box was traceable to ‘freetvstat.iptv.infomir.com.ua’” and “streamed through a website owned by Infomir.” Pl. Mem. dated June 24, 2016 (Dkt. No. 81), at 7, 14. Therefore, plaintiffs argued, “the entire factual basis of Infomir's motion – that Infomir is nothing more than an innocent hardware supplier – is demonstrably false.” *Id.* at 8. Plaintiffs urged the Court to give them leave to replead their claims against Infomir in more detail, using the “facts set forth in the Vidulich Aff.” *Id.* at 14.

After reviewing the Vidulich Affidavit, I recommended that plaintiffs be granted leave to amend and that Infomir's motion to dismiss be denied as moot. *See* Report and Recommendation dated Feb. 15, 2016 (Dkt. No. 181), at 6, 30. On March 27, 2017, the Hon. George B. Daniels, United States District Judge, adopted my recommendation, granted plaintiffs' motion to amend, and denied Infomir's motion to dismiss as moot. (Dkt. No. 201.)

G. Plaintiffs' First Amended Complaint and Summary Judgment Motions

In the First Amended Complaint, filed on April 5, 2017, plaintiffs attach and expressly rely on the Vidulich Affidavit to support their claim that Infomir re-transmits plaintiffs' channels via IPTV, in violation of the FCA, the Copyright Act, the Lanham Act, and the GBL. FAC ¶¶ 1-2, 115, 196, 204-15, 220-45, 262-316. *See also id.* ¶ 197 & Ex. 15 (alleging that the Vidulich Affidavit “detail[s] Infomir's unlawful conduct”). In addition, plaintiffs once again assert that the Infomir brand STBs are “primarily designed for the purposes of circumventing the Broadcasters' technological measures controlling access to Broadcasters' copyrighted works,” *id.* ¶ 256, such

that the sale of these products, in and of itself, violates § 604(e) of the FCA and the DMCA, 17 U.S.C. § 1201(b). FAC ¶¶ 1, 2, 116, 118-20, 216-19, 246-61. Thus, plaintiffs allege, “the Infomir Defendants *both* operate a pirate streaming service *and* manufacture and sell equipment and software designed to assist and profit from other pirates.” *Id.* ¶ 1 (emphasis added).⁷

Since the filing of the FAC, plaintiffs’ senior executives have repeatedly vouched for the Vidulich Affidavit and its conclusions. Alexander Shprekher, the Deputy CEO and Head of Strategy and Business Development for lead plaintiff Joint Stock Company Channel One, declared under penalty of perjury on March 23, 2018 that the facts asserted in the Vidulich Affidavit “are true.” Shprekher Decl. (Dkt. No. 550) ¶ 7; *see also id.* ¶ 55 (“a review of the [Vidulich Affidavit] clearly shows an unauthorized Ukrainian source for Infomir’s streams to the U.S.: freetvstat.iptv.infomir.com.ua”).⁸ A few weeks later, senior executives at Limited Liability Company “Rain TV-Channel,” Limited Liability Company Global Entertainment TV, and CTC Media (the parent company of Closed Joint Stock Company CTC Network, Closed Joint Stock Company TV DARIAL, and Closed Joint Stock Company “New Channel”) similarly affirmed,

⁷ The “Infomir Defendants,” as that term is used in the FAC, include Infomir itself, Teletec, a German entity called Infomir GmbH, and two individuals. *See* FAC at 1, ¶¶ 30-34. On January 3, 2018, plaintiffs voluntarily dismissed their claims against Teletec and the two individuals. (Dkt. No. 492.) On September 28, 2018, acting on my recommendation, Judge Daniels dismissed plaintiffs’ claims against Infomir GmbH for lack of personal jurisdiction. (Dkt. No. 675.) Only one “Infomir Defendant” – the New York LLC – remains a party to this action.

⁸ The top level domain “.ua” is Ukrainian. Shprekher Decl. ¶ 55. This is apparently the basis for Shprekher’s assertion that the server freetvstat.iptv.infomir.com.ua – which Vidulich identified as the source of the pirated Channel One broadcast he viewed during the Wireshark Investigation – was “located in Ukraine.” *Id.* Vidulich himself, however, attested that the IP address for freetvstat.iptv.infomir.com.ua was 66.234.224.2 and that it was “located within the United States.” Vidulich Aff. ¶ 25. Shprekher did not address this discrepancy.

under oath, that the facts stated in the Vidulich Affirmation “are true.” Sindeeva Decl. (Dkt. No. 574-1) ¶ 6; Chistov Decl. (Dkt. No. 574-2) ¶ 8; Kostyuk Decl. (Dkt. No. 574-3) ¶ 7.

In addition, plaintiffs relied on the Vidulich Affidavit to support two separate motions for summary judgment against Infomir, each of which they later withdrew. *See* Pl. Mem. dated May 23, 2017 (Dkt. No. 269), at 14 (“the Programming was streaming from, among other sources, ‘freetvstat.iptv.infomir.com.ua’”), *motion withdrawn* by Order dated February 9, 2018 (Dkt. No. 522); Pl. Mem. of Law dated March 23, 2018 (Dkt. No. 547), at 6 (“Broadcasters have tracked U.S. video streams of pirated Channel One programming viewed on Infomir STBs to an Infomir affiliated server, freetvstat.iptv.infomir.com.ua, located in Ukraine.”); *motion withdrawn* by Order dated October 9, 2018 (Dkt. No. 679).

H. Plaintiffs Fail to Produce the Channel One PCAP

The parties were required to exchange their initial disclosures pursuant to Fed. R. Civ. P. 26(a)(1)(A) on May 3, 2017. (Dkt. No. 236.) Despite plaintiffs’ repeated reliance on the Vidulich Affidavit, they failed to produce the Channel One PCAP (or any other Wireshark ESI) at that time. Nor did they produce those materials in response to Infomir’s May 3, 2017 document requests, which asked for documents “relating to any inspection, test or examination of any device alleged to be originating from or the responsibility of Infomir.” *See* Infomir Ltr. dated Feb. 6, 2018 (Dkt. No. 516), at 2; *id.* Ex. A, Doc. Req. No. 56. Thus, as of February 6, 2018 – nine months after the document requests were served, and less than six weeks before fact discovery was then scheduled to close (*see* Amend. Case Mgmt. Order (Dkt. No. 429) ¶ 2) – plaintiffs had produced *no* documents concerning the Wireshark Investigation other than the Channel One Screenshots.

Infomir Ltr. dated Feb. 6, 2018, at 2; Infomir Mem. dated Nov. 5, 2018 (Infomir Moving Mem.) (Dkt. No. 693), at 8.

During a discovery conference on February 9, 2018, Infomir sought documents and information concerning Vidulich's May 2016 investigations. I directed plaintiffs to turn over the usernames and passwords that Vidulich used to conduct his investigations, so that defendants could "trace his footsteps" and "double-check that he did what he said what he did." 2/9/18 Conf. Tr. (Dkt. No. 529) at 82:24-83:11, 90:17-21. Infomir's attorney then sought an order compelling plaintiffs to supplement their production in response to document request No. 56, limited to tests that "plaintiffs, not their attorneys, have done, tests, examination, inspection, et cetera with respect to any hardware that they allege is ours." *Id.* at 121:15-19. I granted the application and directed plaintiffs to provide a supplemental response to No. 56, "with respect to any hardware testing conducted not by counsel or by an expert under counsel's direction but by the client." *Id.* at 121:21-24. *See also* Order dated Feb. 13, 2018 (2/13/18 Order) (Dkt. No. 524), ¶¶ 5, 7(a).

I. The Vidulich Subpoena

On March 23, 2018, plaintiffs filed their second summary judgment motion, which relied on the Vidulich Affidavit to establish that Channel One's programming was unlawfully streamed into the United States from "an Infomir affiliated server, freetvstat.iptv.infomir.com.ua, located in Ukraine." Pl. Mem. of Law dated March 23, 2018, at 6. On April 16, 2018, in a joint letter updating the Court on the parties' discovery disputes, Infomir advised that it had "noticed the deposition of Mr. Vidulich," and sought an order compelling plaintiffs to disclose "the electronically stored data from the 'network protocol analyzer' referenced in Mr. Vidulich's affidavits." Joint Ltr. dated Apr. 16, 2018 (Dkt. No. 566), at 4; *see also* Vidulich Subpoena (Dkt. No. 711-5) at ECF page 5 (seeking

“[a]ny and all documentation related to, and data collected from, the ‘network protocol analyzer’ you used in your alleged 2016 investigation”).

Plaintiffs opposed the request, arguing that the Vidulich deposition subpoena constituted “dilatory harassment of a paralegal,” and that any ESI generated by his Wireshark Investigation would be protected from discovery by the work product doctrine. Joint Ltr. dated Apr. 16, 2018, at 5. At the same time, however, plaintiffs offered “to allow a forensic investigator to inspect the devices used by Mr. Vidulich at a date and time agreed upon by the parties.” *Id.*

At a discovery conference on April 19, 2018, I advised the parties that Vidulich was “a fact witness who can be examined at deposition on matters of fact,” including “his actual investigatory activities,” but “not his strategic communications or directions or reports” to Dunnington. 4/19/2018 Conf. Tr. (Dkt. No. 570) at 95:8-19. Infomir then pressed its request for “all of the data that came out of that [May 2016] investigation. The most obvious piece of that is a data file that was generated when Mr. Vidulich used what you called a network analyzing program.” *Id.* at 97:2-5. Infomir noted that only screenshots had been produced thus far and explained, “We want to see – and I think we’re entitled to see the full data file” generated during the May 27, 2016 Wireshark Investigation. *Id.* at 97:8-10. One of plaintiffs’ lawyers, Dunnington partner Samuel Blaustein, agreed to “extract” that data from the Firm Laptop with the help of “our in-house person” or, if necessary, “perhaps an outside source.” *Id.* at 99:20-100:10.

J. The April 25, 2018 Order

In a written Discovery Order dated April 25, 2018 (4/25/18 Order) (Dkt. No. 569), I directed plaintiffs to produce Vidulich for deposition and reiterated that he could be examined concerning “the facts concerning the websites, apps, and software he accessed or utilized, the

observations he made when he did so, and the information and data he acquired as a result of these activities.” 4/25/18 Order at 4. In addition, I directed plaintiffs to produce:

any additional documents in their possession, custody, or control (beyond those attached as exhibits to the witness’s various declarations) constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities. These documents are responsive to Infomir’s Document Request No. 56 and are not themselves privileged.

Id. at 5. The fact discovery deadline was extended to May 31, 2018 to accommodate the Vidulich deposition and related document production, as well as certain other discovery. *Id.* at 12.

On May 9, 2018, plaintiffs objected to the 4/25/18 Order pursuant to Fed. R. Civ. P. 72(a), arguing that “[t]he deposition of Dunnington paralegal Christopher Vidulich is pure harassment to run up legal costs.” Pl. Mem. dated May 9, 2018 (Dkt. No. 581), at 6. On June 12, 2018, the district judge overruled plaintiffs’ objections. (Dkt. No. 605.)

K. The June 26, 2018 Conference

Plaintiffs did not produce Vidulich for deposition by May 31, 2018. Nor did they produce the Channel One PCAP – or any other ESI “constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities,” as directed by the 4/25/18 Order. *See* Joint Ltr. dated Jun. 15, 2018 (Dkt. No. 611), at 3, 12.

On June 22, 2018 – three weeks past the deadline set by the 4/25/18 Order – plaintiffs produced a document that they described as “an output data file for a Wireshark search that Christopher Vidulich completed on May 24, 2016.” Leviss Decl. dated Nov. 5, 2018 (Dkt. No. 694), Ex. C. The Vidulich Affidavit described a Wireshark investigation performed three days later, on May 27, 2016. Plaintiffs did not comment on the date discrepancy. Nor did they explain

why the “output data” was produced as an “XPS” file with the extension “.xps” (the Channel One XPS), but not as a PCAP file (with the extension “.pcap”), which is Wireshark’s native format.⁹

On June 26, 2018, during another discovery conference, Infomir noted that the Channel One XPS and the Channel One PDF appeared to relate to a May 24, 2016 Wireshark investigation rather than the May 27, 2016 investigation described in the Vidulich Affidavit, and complained that plaintiffs would not “clarify whether there were other investigations, whether they’re going to give us the data from the May 27th investigation, whether this is exclusive, or why we can’t get the Wireshark data” underlying the investigation described in the Vidulich Affidavit. 06/26/2018 Conf. Tr. (Dkt. No. 694-7) at 136:9-18. One of plaintiffs’ attorneys, Dunnington associate Hardin Rowley, assured the Court that “[a]ll the documents [Vidulich] created have been produced,” *id.* at 137:8-9, *see also id.* at 138:23-139:3, adding that Dunnington was only able to extract “one file” from the Firm Laptop, presumably meaning the Channel One XPS, “and that’s all we were able to get.” *Id.* at 137:12-13; *see also id.* at 139:22-23 (“We did the search of the laptop last week, and we provided them with the file we found.”).

⁹ When plaintiffs produced the Channel One XPS they also included a version of the same document converted to Portable Document Format with the extension “.pdf” (the Channel One PDF). Leviss Decl. Ex. C. “XPS” is a Microsoft file format which (according to non-Microsoft sources) was intended to be “Microsoft’s alternative to PDF” but “never gained much traction.” Chris Hoffman, *What Is an XPS File, and Why Does Windows Want Me to Print to One?*, How-To Geek (July 5, 2017, 11:44 AM), <https://www.howtogeek.com/148499/what-is-an-xps-file-and-why-does-windows-want-me-to-print-to-one/>. “An XPS file represents a document with a fixed layout, just as a PDF file does.” *Id.* As discussed in more detail below, neither an XPS file nor a PDF file contains “all of the data” recorded during a Wireshark capture. Rucinski Rep. at 7. The “full data payload,” including “the actual text and video data that was received during the Wireshark capture,” is preserved only in the native format PCAP file created when the capture occurs. *Id.* at 9.

Plaintiffs did not address the date discrepancy. They did, however, offer again to produce the Firm Laptop for examination, 06/26/2018 Conf. Tr. at 137:16-18, and I gave Infomir a deadline to respond. *Id.* at 140:9-141:13. On June 29, 2018, Infomir reported that it had hired Stroz Friedberg to image the laptop and perform a forensic analysis. (Dkt. No. 615.)

L. The July 3, 2018 Order

Following the June 26 conference, I issued a written Order, dated July 3, 2018, directing plaintiffs to “conduct a further search of their records, including ESI, and [] produce any additional documents constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities.” 7/3/18 Order (Dkt. No. 617) ¶ 7. Noting that plaintiffs had not yet produced any data from the May 27, 2016 Wireshark Investigation, I stressed the importance of that data – to back up plaintiffs’ claim that “Infomir was involved in ‘content distribution activity’” – and directed plaintiffs to complete their search and produce all remaining documents by July 10, 2018. *Id.* I specifically warned plaintiffs that Infomir’s forensic analysis of the Firm Laptop, which was underway, “does not relieve plaintiffs of their obligation, set forth above, to produce any additional documents constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities no later than July 10, 2018.” *Id.* ¶ 8. The 7/3/18 Order directed the parties to complete the Vidulich deposition by July 31, 2018. *Id.* ¶ 9.

On July 9, 2018, plaintiffs produced “[a]dditional screenshots and .pdfs that were not included with any of Mr. Vidulich’s prior affidavits.” Leviss Decl. Ex. D. This production included another version of the Channel One PDF (regarding the May 24, 2016 capture) but nothing from May 27, 2016, and no native-format PCAP files. Leviss Decl. ¶ 6.

On July 13, 2018, in accordance with a Stipulated Order that the parties negotiated to govern Infomir's examination of the Firm Laptop (Dkt. No. 626), Stroz Friedberg sent Dunnington a list of the Wireshark-related "search hits" it found on the Firm Laptop. *See* Tr. of Feb. 6, 2019 Hr'g (Hr'g Tr.) (Dkt. No. 733), at 8. The list included the full name and file path of the Channel One PCAP: "c:\Wireshark\Channel One Capture.pcapng." Pl. Ltr. dated Oct. 18, 2018 (Dkt. No. 686), at 2; *id.* Ex. A, at ECF page 2. The list also noted that this file was no longer "existent." *Id.*

M. The Vidulich Deposition

On August 29, 2018, Vidulich testified at deposition that the Wireshark capture described in his affidavit occurred on May 27, 2016; that he "never did Wireshark" other than for that investigation; that he did not "save the Wireshark capture data" except "[a]s a screen shot"; and that he personally took the Channel One Screenshots. Vidulich Dep. Tr. (Leviss Decl. Ex. B) at 25:18-20, 28:4-19, 32:1-25, 98:13-14.

Asked to explain his conclusion that the STB "had a connection with Infomir," Vidulich pointed to packet 72 on the Channel One Screenshot attached to his affidavit as Exhibit 14, which – he said – showed that the STB was connecting to the IP address 66.234.224.2. Vidulich Dep. Tr. at 43:9-23. "Then in the info section it says standard query, freetvstat.ipvtv.infomir.com.ua." *Id.* at 43:17-19. Vidulich said he found that line after "capturing for maybe 30 seconds," then pausing the program and scrolling through the lines of code until "[he] found Infomir," at which point he used his "snipping tool" to create the screenshot. *Id.* at 44:2-11. Vidulich confirmed that packet 72 was "almost 23 seconds in" to the capture, as signified by the timestamp 22.970968. *Id.* at 44:15-20. He knew that he was actually "connecting to the stream" on May 27, 2016, because "[he] was viewing Channel One at that time." *Id.* at 46:7-15; *see also id.* at 73:16 ("the Channel One stream

was active”). Vidulich paused the capture for “[l]ess than five minutes” to take the snippet. *Id.* at 47:19-22.

Towards the end of the deposition, Vidulich was asked whether he deleted “any of the Wireshark information” from the Firm Laptop:

A. I didn't delete anything.

Q. Are you aware if the Wireshark capture[] data, that you described in your affidavit remains on the laptop computer that you used?

A. I don't think it's there.

Q. Do you know what happened to it?

A. It wasn't saved.

Vidulich Dep. Tr. at 98:19-99:4; *see also id.* at 99:17-21 (testifying that the Wireshark data referred to in the Vidulich Affidavit was not, to his knowledge, saved “on any computer”).

When Infomir's counsel asked Vidulich whether he created the Channel One XPS recently produced by plaintiffs (and dated May 24, 2016), Vidulich said “no,” adding, “I think it was auto-saved.” *Id.* at 28:20-29:1. Thereafter, when Vidulich was asked about the “source” of that Channel One XPS, plaintiffs' lead counsel, Raymond J. Dowd, instructed him not to answer on the ground that the question went “way outside the scope of his declarations.” *Id.* at 99:5-16.¹⁰

¹⁰ During the deposition, which lasted two hours and 13 minutes, attorney Dowd instructed Vidulich not to answer at least 29 times. *See* Vidulich Dep. Tr. at 4-5. Counsel refused to permit the witness to reveal (among other things) where he got the Infomir brand STBs he used in his investigation, whether they had been used before he used them; whether they had been altered; or even whether the Mag 254 STB “was in a carton or packaging” when he first used it. *Id.* at 36:20-23, 41:20-24, 65:17-66:12, 74:1-15, 79:2-3. In addition, counsel instructed Vidulich not to disclose how he learned to interpret Wireshark data, *id.* at 10:23-11:12, whether he had ever conducted any Wireshark investigations other than the May 27, 2016 investigation described in the Vidulich Affidavit, *id.* at 26:18-28:2, or whether he did anything to determine if the information to which he swore was accurate. *Id.* at 61:17-24.

N. Infomir's Request for Leave to Seek Spoliation Sanctions

By letter dated September 14, 2018, Infomir reported – based in part on the work of Stroz Friedberg – that the Channel One XPS and the Channel One PDF, although dated May 24, 2016, contained data exactly “matching the network protocol analysis and investigation that Vidulich claims to have engaged in on May 27, 2016,” as reflected in the Channel One Screenshots. Infomir Ltr. dated Sept. 14, 2018 (Dkt. No. 657), at 3. Further, “[t]he forensic examination of the laptop confirms that wireshark data, in native .pcap format, was at one time saved to the laptop and was subsequently deleted before the laptop was produced for defendants’ examination.” *Id.* Thus, Infomir explained, Vidulich’s testimony – that the Wireshark data he captured was never saved – was “demonstrably false,” *id.*; in fact, the native-format Wireshark data “was saved, converted to a non-native format, ‘cleansed’ by being saved to a fixed format (pdf/xps) and then deleted.” *Id.* (emphasis in the original). As discussed in more detail below, all of these charges proved to be accurate – except that the Channel One PCAP was not, in fact, permanently deleted.

Infomir sought leave to move for spoliation sanctions up to and including dismissal:

The intentional deletion of this critical and previously saved computer data file documenting the activity which plaintiffs rely upon as the foundation for their claims against Infomir, LLC, is the definition of spoliation of evidence. No sanction short of dismissal of this lawsuit can level the playing field given plaintiffs' intentional destruction of the foundational evidence of their lawsuit.

Infomir Ltr. dated Sept. 14, 2018, at 3.

O. The September 21, 2018 Vidulich Affidavit

In a sharply-worded responding letter signed by attorney Dowd, supported by a newly-executed affidavit from Vidulich, both dated September 21, 2018, plaintiffs claimed that the Channel One XPS was created during an “unrelated preliminary investigation” that was conducted on May 24, 2016, was “never filed by Broadcasters,” and was therefore “irrelevant” to the validity

of the Vidulich Affidavit or the May 27, 2016 investigation described therein. Pl. Ltr. dated Sept. 21, 2018 (Dkt. No. 666), at 3; 6/21/18 Vidulich Aff. (Dkt. No. 666-2) ¶¶ 14-15. Plaintiffs insisted that Vidulich conducted the “relevant” Wireshark Investigation on May 27; that he did not save any data from that investigation, except in the form of the Channel One Screenshots; that they had already produced “everything that was retained”; and that “[n]othing was spoliated.” Pl. Ltr. dated Sept. 21, 2018, at 3; 9/21/18 Vidulich Aff. ¶¶ 6-7, 11. Vidulich added that, due to his lack of technical expertise, “I did not even know how to properly save Wireshark data, let alone what the native format of Wireshark data is.” *Id.* ¶ 13.

As discussed in more detail below, all of these statements proved to be false – except, as noted above, that the Channel One PCAP was not, in fact, permanently deleted.

P. The October 5, 2019 Conference

During a conference on October 5, 2018, Infomir explained in more detail why it believed that Vidulich saved, but then deleted, the native-format PCAP file underlying his original affidavit: First, the upper left-hand corner of both Channel One Screenshots showed that a PCAP file named “Channel One Capture.pcapng” was open when those screenshots were created. 10/5/18 Tr. (Dkt. Nos. 682, 694-8) at 48:4-25. Second, “on the laptop there is a remnant of a Wireshark search in PCAP that had been saved at one point in time and was no longer there.” *Id.* at 51:11-13. Moreover, Infomir added, the Channel One XPS did not reflect a “different search on a different day,” because the data shown in that file “lines up exactly to all the IP addresses to the millionth of a second” with the Channel One Screenshots. *Id.* at 52:14-21.

In short, Infomir believed, based on the information then available to it, that plaintiffs conducted a single Wireshark investigation, likely on May 24, 2016, evidenced by (i) a native

format PCAP file named “Channel One Capture.pcapng,” which was created during the original investigation and saved to the Firm Laptop, but deleted before the laptop was turned over for forensic analysis; (ii) the “fixed layout” Channel One XPS and Channel One PDF, also created on May 24, 2016, but first produced more than two years later, on June 22, 2018; and (iii) the Channel One Screenshots, which appeared to have been created three days later on May 27, 2016, and showed only a “snippet” of the data collected by Wireshark.

In response, attorney Dowd once again insisted that plaintiffs had turned over “[e]verything that was saved or screen shotted.” 10/5/18 Tr. at 67:6-15. The Court then set a briefing schedule for Infomir’s motion and otherwise stayed expert discovery pending the resolution of that motion. 10/5/18 Tr. at 80:21-25; *see also* Order dated Oct. 9, 2018 (Dkt. No. 679), ¶¶ 4-5.

Q. The Channel One PCAP and the October 12, 2018 Vidulich Affidavit

One week later, on Friday afternoon, October 12, 2018, plaintiffs produced the Channel One PCAP, “which consists of a .pcapng file dated May 24, 2017.” Pl. Ltr. dated Oct. 12, 2018, Ex. 1 (Dkt. No. 686-2, at ECF page 7). That same day, plaintiffs produced yet another affidavit from Vidulich, who attested that on June 22, 2018, in anticipation of complying with the 4/25/18 Order, he transferred the Channel One PCAP from the Firm Laptop to his desktop computer, where it was somehow overlooked. 10/12/18 Vidulich Aff. (Dkt. No. 686-2, at ECF pages 4-5) ¶¶ 4-7.

According to Vidulich, he first “locate[d] all data relating to [his] 2016 investigations” on the Firm Laptop. 10/12/18 Vidulich Aff. ¶ 4. He then used a UBS flash drive to “transfer” those files onto his desktop computer at Dunnington, so that he could “produce the files to Infomir.” *Id.* ¶ 5. Vidulich swore that he did not “delete” the Channel One PCAP, *id.* ¶ 6, but could not explain why it “was not on the laptop” when that laptop was turned over for forensic examination. *Id.* ¶ 11.

Once the PCAP file was moved to his desktop, Vidulich was not “able to open” it. 10/12/18 Vidulich Aff. ¶ 7. This was apparently why it was not produced to Infomir along with the Channel One XPS. Indeed, according to plaintiffs’ designated Wireshark investigator, he did not know, at the time, “that the native file format for a Wireshark capture is ‘.pcap.’” *Id.* ¶ 8.

Insofar as the record discloses, Vidulich did not seek any assistance in opening the PCAP file, nor in understanding what it was. Rather, according to Vidulich, he first learned what a PCAP file was when he reviewed Infomir’s September 14, 2018 letter seeking leave to move for spoliation sanctions. 10/12/18 Vidulich Aff. ¶ 8. Even that, apparently, did not prompt any renewed efforts to retrieve the Channel One PCAP. Vidulich does not describe any such efforts until after the October 5, 2018 court conference, when attorney Rowley asked him to review the files he had transferred to his desktop computer. *Id.* ¶ 9. Plaintiffs then produced the Channel One PCAP. *Id.* ¶ 10.¹¹

Plaintiffs immediately demanded that Infomir withdraw its (not yet filed) motion for spoliation sanctions, explaining that the “omission” of the Channel One PCAP from its productions was “inadvertent” and complaining that Infomir “created” the “purported ‘spoliation’ issue” by failing to conduct its forensic analysis of the Firm Laptop when first offered the opportunity to do

¹¹ Nowhere in the 10/12/18 Vidulich Affidavit – or in any of his prior affidavits – did he acknowledge that he had received any training or had access to any expert advice regarding the Wireshark program. To the contrary: Vidulich repeatedly attested that he had no “specialized technical knowledge” and had “never studied computer science, information technology, Internet Protocol Television (‘IPTV’) or network protocol analyzers.” 10/12/18 Vidulich Aff. ¶ 2. *See also* Vidulich Aff. ¶ 2; 9/21/18 Vidulich Aff. ¶ 2; *id.* ¶ 21 (attesting that at the time he conducted the Wireshark Investigation, he “had less than five months of experience in the legal profession and a grand total of zero months of experience in network protocol analysis”).

so in April. Pl. Ltr. dated Oct. 12, 2018 (Dkt. No. 686-2), at 1. Plaintiffs also faulted Infomir for failing to “specifically request[]” any “potentially missing .pcap files” until September. *Id.* at 2.

R. The October 19 Conference

The production of the Channel One PCAP prompted another round of letter-motions. Infomir asked for confirmation that the Channel One PCAP was in fact “the data viewed and relied upon by Mr. Vidulich” during the investigation reported in his original affidavit. Infomir Ltr. dated Oct. 16, 2018 (Dkt. No. 684), at 1.¹² Plaintiffs refused to answer Infomir’s question. *See* Pl. Ltr. dated Oct. 18, 2018 (Dkt. No. 686), at 1-5. Instead, plaintiffs accused Infomir of a wide range of misconduct – including, bizarrely, obtaining an “unauthorized” expert report from Stroz Friedberg regarding its forensic analysis of the Firm Laptop, *id.* at 1 – and requested that the Court compel Infomir to turn over that report, together with “all communications with its expert,” and “conclusively determine that there was no spoliation.” *Id.* at 1, 5.

During an October 19, 2018, telephonic conference, I asked plaintiffs’ counsel the same question that Infomir posed in its correspondence: “Mr. Blaustein, is this it?” 10/19/18 Tr. (Dkt. No. 694-5) at 7:16. Counsel could not or would not say. “Your Honor, I can’t definitely state as a layperson, much like Mr. Vidulich is a lay witness, whether this PCAP file is it.” *Id.* at 7:17-20. Counsel represented, however, that “there are no other native PCAP” files, and conceded that the

¹² Infomir explained that if in fact there was only one Wireshark capture, which occurred on May 24, then Vidulich’s claim to have performed the capture on May 27 was “materially false,” not only with respect to the date but also with respect to how he went about the investigation. Infomir Ltr. dated Oct. 16, 2018, at 2. Alternatively, Infomir argued, “[i]f there are in fact two sets of Wireshark data from two different dates, plaintiffs must account for the missing May 27, 2016 data.” *Id.* at 2-3.

“logical inference” was that there was no Wireshark search conducted on May 27, 2016; “[t]here was only the search conducted on May the 24th.” *Id.* at 17:2-18.

Infomir sought leave to re-depose Vidulich, explaining that with the production of the Channel One PCAP “[t]he issue now is probably not one of spoliation but is more likely one of . . . submissions to the court that are not factually supported,” which would also warrant sanctions, “albeit not [for] spoliation.” *Id.* at 18:18-19:25. I denied leave to take a second pre-motion deposition, *id.* at 20:6-23, and set a new briefing schedule for Infomir’s sanctions motion. *Id.* at 24:12-15; *see also* Order dated Oct. 19, 2018 (Dkt. No. 688), ¶¶ 1-2.

II. THE SANCTIONS MOTION

A. Infomir’s Moving Papers

Infomir filed its motion on November 5, 2018, pursuant to Fed. R. Civ. P. 37(b) and the Court’s inherent equitable powers, seeking an order “precluding plaintiffs from presenting or utilizing in this action, in any manner, any aspect of the May 2016 investigation.” Infomir Moving Mem. at 2. Infomir argues that plaintiffs engaged in serious and sustained discovery misconduct, including (i) repeated violations of court orders that required the production of the Channel One PCAP; (ii) false statements by Vidulich and by plaintiffs’ counsel; and (iii) related obstructive conduct, such as delaying Vidulich’s deposition and instructing him not to answer unobjectionable questions, all designed to prevent Infomir from discovering – with the assistance of the Channel One PCAP – that key portions of the Vidulich Affidavit “are not true.” *Id.* at 1, 22-23.

Infomir contends that it was deeply prejudiced by the misconduct (above and beyond the expense incurred in uncovering the truth) because it was required to respond to the First Amended Complaint and complete fact discovery, including depositions, without the data from which it

could have challenged the central factual assertions on which plaintiffs’ “streaming” case was built. Infomir Moving Mem. at 12-13, 21-22. Therefore, Infomir argues, preclusion is the appropriate sanction, because it “expunges the tainted ‘evidence’ from the case” while preserving “plaintiffs’ ability to develop evidence of the alleged ongoing streaming through qualified experts” who could then be cross-examined as to their “knowledge, methodologies and conclusions.” *Id.* at 2. Infomir also seeks an award of its fees and other expenses incurred in uncovering the Channel One PCAP, *id.* at 22, 26, but urges that monetary sanctions alone would not be sufficient to ameliorate the prejudice it has suffered or “deter future misconduct,” particularly given that plaintiffs’ litigation costs are underwritten by a third party, rendering plaintiffs “immune from the normal financial incentives governing good faith litigation.” *Id.* at 22.

In the accompanying Rucinski Report, Infomir demonstrates that the Channel One Screenshots, the Channel One XPS, the Channel One PDF, and the Channel One PCAP were all generated from a single Wireshark capture that occurred on May 24, 2016. Rucinski Rep. at 3, 4, 7, 12. Although the screenshots self-authenticate as having been taken on May 27, 2016, *id.* at 7, they too reflect data gathered from the capture performed three days earlier, meaning that Vidulich was not watching a “live” stream when he took those screenshots. *Id.* Thus, Vidulich’s oft-repeated statements “about conducting a separate Wireshark investigation on May 27, 2016 to which he attributes the Channel One Screenshots” were, in Rucinski’s words, “inconsistent with and unsupported by the available data and evidence.” *Id.* Similarly, the statements by Vidulich and by plaintiffs’ counsel after the Channel One XPS surfaced – that an “unrelated preliminary investigation” was conducted on May 24 – were “incorrect.” *Id.* Moreover, if Vidulich was telling the truth when he testified that he personally “did Wireshark” only once – on May 27 – then “he

did not perform the May 24, 2016 Wireshark capture,” *id.* at 12; rather, he viewed a previously-recorded capture conducted and saved by someone else. That someone else, Infomir suggested, could have been “someone from Kartina with technical expertise,” who was “remotely accessing Vidulich’s laptop computer during the May 2016 investigation process.” *Id.* at 17.

Although all of the Wireshark-related ESI ultimately produced by plaintiffs relates to the same capture, only the Channel One PCAP constitutes the “saved native data captured by the Wireshark program,” and only the Channel One PCAP “contains all of the data that was recorded by Wireshark as part of that capture in a format that can be fully and easily analyzed.” Rucinski Rep. at 7, 12. Data is sent over the internet in “packets.” *Id.* at 1. The Channel One Screenshots show limited information about 24 packets (out of 2087 total packets captured during the entire May 24 investigation). *Id.* at 4. The Channel One XPS shows all 2087 packets, but, like the screenshots, displays only a “subset” of the available information for each. *Id.* The Channel One PCAP, however, contains “all of the data that was recorded by Wireshark,” including “the full detail of the HTTP information in the packet” and “the actual text and video data that was received during the Wireshark capture,” which are “not present” in any of the other ESI produced by plaintiffs. *Id.* at 8-9; *see also id.* at 9 (only the PCAP file “contains the full payload that gets sent or received”).

Based on his analysis of the Channel One PCAP, Rucinski states that most of the conclusions that Vidulich drew from the Channel One Screenshots were simply wrong. For example, according to Rucinski, packets 72 and 73 do *not* show that the Infomir STB was “communicating” with “freetvstat.iptv.infomir.com.ua,” nor that “freetvstat.iptv.infomir.com.ua” had the IP address 66.234.244.2. Rucinski Rep. at 10. Rather, packet 72 shows a request from the

STB to a “DNS” (Domain Name System) server at the IP address 66.234.244.2, asking for information *about* “freetvstat.iptv.infomir.com.ua.” *Id.* Packet 73 “is the response from the DNS Server,” which refused the request. *Id.* Packets 74 and 75 (not mentioned by Vidulich) show the STB querying a different DNS server for information about “freetvstat.iptv.infomir.com.ua” and learning that its IP address was 79.142.197.4. *Id.* at 10-11.

Perhaps most importantly, “The domain ‘freetvstat.iptv.infomir.com.ua’ was not the source of IPTV video data captured in Channel One PCAP.” Rucinski Rep. at 11. Rucinski explains:

Less than 1% (17 of 2,078) of the packets in the Channel One PCAP are sent to or from, the IP address of “freetvstat.iptv.infomir.com.ua,” and less than 2% (2033 bytes of 1779 kilobytes) of the IP data sent to the [Infomir] STB . . . in the Channel One PCAP originated from 79.142.197.4. There are only seven packets in Channel One PCAP that contain data sent from the 79.142.197.4 IP address (packets 78, 81, 82, 287, 305, 557, and 577). I have manually inspected the full content of each of these packets using Wireshark; none of them contain video data.

Id. Rucinski adds that the Infomir STB was not receiving *any* video content, from *any* source, via packet 72 – or any of the other packets referenced in the Vidulich Affidavit or shown in the attached Channel One Screenshots. *Id.*

B. Plaintiffs’ Opposition Papers

In their opposition papers, plaintiffs do not dispute the key conclusions drawn by Infomir’s expert concerning the inaccuracies in the Vidulich Affidavit. To the contrary: they now concede that Vidulich conducted the Wireshark capture described in the Vidulich Affidavit on May 24, 2016, saved that data as the Channel One PCAP, and used the Channel One PCAP three days later, on May 27, to generate the screenshots attached to his affidavit. *See* Pl. Opp. Mem. dated Dec. 20, 2018 (Dkt. No. 714), at 3; Dietrich Decl. ¶¶ 7, 34-36, 73 (Vidulich’s “May 27, 2016 screenshots were of the Wireshark capture that took place on May 24, 2016”). In his latest affidavit, filed along with plaintiffs’ opposition brief, Vidulich himself acknowledges that “[t]he Wireshark data which

I reference in my affidavit sworn to on June 24, 2016 (ECF 80) was captured on May 24, 2016. On May 27, 2016, I took screenshots of the Wireshark data that I had previously captured in order to attach it to my affidavit.” 12/20/18 Vidulich Aff. (Dkt. No. 713) ¶ 7; *see also id.* ¶ 13 (“The May 27, 2016 screenshots attached to my June 2016 affidavit are true and accurate recordings of the data collected on May 24, 2016.”).

Plaintiffs’ opposition papers also answer some of the questions that attorney Dowd refused to permit Vidulich to answer at deposition. For example, Vidulich discloses that he was taught how to use Wireshark by “Dmitri Dietrich, Chief Technology Officer of Kartina Digital GmbH.” 12/20/18 Vidulich Aff. ¶ 5. Both Vidulich and Dietrich state that Dietrich and his “technical support team” at Kartina conducted an instructional session with Vidulich on May 19, 2016, via Skype and a program called TeamViewer, which allows the instructor to take remote control of the pupil’s computer. Dietrich Decl. ¶ 78; 12/20/18 Vidulich Aff. ¶ 5. During that session, Dietrich taught Vidulich “how to capture data transfers of an STB and how to interpret and analyze such transfers.” Dietrich Decl. ¶ 78. Dietrich also “guided Mr. Vidulich on how to configure the hardware” for the Wireshark Investigation. *Id.* ¶ 21.¹³

Plaintiffs do not explain why they so persistently insisted – in Vidulich’s case, under oath – that he conducted the capture and took the screenshots on the same day, May 27, 2016; that “the Channel One Stream was active” when he viewed it on May 27; that he did not save any of the data he captured, other than in screenshot form; and that did not even know how to do so. Nor do

¹³ Vidulich denies, however, that his computer was remote-controlled by Kartina when he performed the Wireshark capture on May 24, 2016. 12/20/18 Vidulich Aff. ¶¶ 11-12.

plaintiffs explain why counsel and investigator alike claimed, falsely, that the Channel One XPS reflected an “unrelated preliminary investigation” that was “irrelevant” to the Vidulich Affidavit.

With regard to “freetvstat.iptv.infomir.com.ua,” Dietrich states only that “the presence of ‘Infomir’ in the domain name indicates that this domain belongs or is related to Infomir.” Dietrich Decl. ¶ 39. He makes no effort to substantiate any of Vidulich’s other statements about that domain or its alleged role in streaming video to the STB. Thus, Dietrich does not defend Vidulich’s assumption that the STB “connected” to “freetvstat.iptv.infomir.com.ua” at packets 72 and 73, his assertion that the IP address for “freetvstat.iptv.infomir.com.ua” was 66.234.244.2, which was “located within the United States,” or his conclusion that “freetvstat.iptv.infomir.com.ua” was the source of the IPTV video data captured in the Channel One PCAP. Similarly, Dietrich does not contest Rucinski’s explanation that no video data (from any source) was transmitted at packets 72-73 – or any of the other packets shown on the Channel One Screenshots.

Instead, Dietrich explains that a different portion of the Wireshark capture – specifically, packet 376, at timestamp 42.529523, which was never reviewed by Vidulich and is not shown in the Channel One Screenshots – reveals, through the “deeper explanatory power” of the Channel One PCAP, that the streaming video was coming from “streamer2de.allfreetv.net,” with the IP address 37.58.59.43. Dietrich Decl. ¶¶ 56-62 & Ex. 6. Dietrich goes on to assert, based on a “domain block search” performed on a third-party website,¹⁴ that the domain “allfreetv.net” is “controlled by Infomir’s servers.” *Id.* ¶¶ 63-66 & Ex. 10. Dietrich therefore concludes (based on information not available until the Channel One PCAP was produced) that the Infomir STB was

¹⁴ Dietrich states that he consulted the website “ipv4info.com,” which revealed that “allfreetv.net” was “listed in Infomir’s domain block search.” Dietrich Decl. ¶ 66 & Ex. 10. Dietrich does not further describe or credential “ipv4info.com.”

in fact “receiving video steaming . . . directly from Infomir’s servers on May 24, 2016,” *id.* ¶ 67, albeit at a different time, via a different packet, and from a different domain, with a different IP address, than the time, packet, domain, and IP address described in the Vidulich Affidavit. In addition, Dietrich asserts that certain other portions of the Vidulich Affidavit were not inaccurate.¹⁵

In their opposition brief and accompanying affidavits, plaintiffs contend that no sanctions are warranted because Infomir failed to comply with Local Civil Rule 37.1, Pl. Opp. Mem. at 1, 15; because none of this Court’s orders “specifically discussed” or required production of “a PCAP,” *id.* at 1, 2, 10, 17; because their failure to produce the Channel One PCAP in response to those orders was “inadvertent,” *id.* at 2, 3, 4; because they “promptly” searched for and “immediately” produced the PCAP file once Infomir “specifically requested” it in September 2018, *id.* at 1, 12, 18, 19, 20, 21; and because they “*fully* obeyed the letter and spirit of the Court’s Orders” by offering Infomir the opportunity to inspect the Firm Laptop. *Id.* at 2 (emphasis in the original), 3-4, 17, 18; *see also* Blaustein Decl. (Dkt. No. 711) ¶¶ 4-5, 8, 22, 31, 33-34, 39, 51, 53-54. Plaintiffs add that the delay in producing the Channel One PCAP was “harmless” because it was “produced in advance of expert discovery.” Pl. Opp. Mem. at 4.

C. Infomir’s Reply Papers

In reply, Infomir’s expert disputes Dietrich’s contention that any portion of the PCAP file shows streaming video coming from an Infomir-controlled domain. *See* Rucinski Supp. Rep. (Dkt.

¹⁵ For example, according to Dietrich, Vidulich correctly observed the STB “had data transfers with Infomir’s Stalker Middleware.” *Id.* ¶ 38. However, Dietrich does not assert that the STB received video content from the Stalker portal during those data transfers.

No. 719-1) at 8-12.¹⁶ He also points out that – right or wrong – Dietrich’s analysis of packet 376 “could not have been developed” without access to the full Channel One PCAP. *Id.* at 6.

In addition, Rucinski asserts that when the Channel One PCAP was saved to the Firm Laptop on May 24, 2016, it must have been “manually saved,” Rucinski Supp. Rep. 5, because its filename was “Channel One Capture.pcapng” rather than the generic sequence of letters and numbers that the Wireshark program would have generated had the file been autosaved. *Id.* 6.

D. The February 6, 2019 Hearing

On February 6, 2019, the Court held an evidentiary hearing. Before the first witness was called, plaintiffs’ lead counsel asserted that while his firm had made “a couple of mistakes,” they were “inadvertent” rather than “disobedient.” Hr’g Tr. at 5-7. According to attorney Dowd, no one at Dunnington knew what a PCAP file was, understood that Infomir expected a PCAP file to be produced, or recognized the significance of the missing “.pcapng” file on the Firm Laptop until months later, in October 2018, when “[w]e found it in the desktop.” *Id.* at 6-10.

When the parties’ respective expert witnesses were called to the stand, they agreed about most of the technical issues relevant to Infomir’s motion. For example, they agreed that the Channel One PCAP was the only complete record of the May 24, 2016 Wireshark capture, *see* Hr’g Tr. at 16, 25-26, 81 (Rucinski), 117-18 (Dietrich), and the only file from which the actual

¹⁶ Rucinski argues that Dietrich’s methodology for tying “streamer2de.allfreetv.net” at the IP address 37.58.59.43 to “Infomir’s servers” was “unreliable,” because, among other things, the domain block search he performed relied upon the IP address 79.142.197.62, which was “not the origin of the video streaming captured in the Channel One PCAP” and “does not appear in the Channel One PCAP at all.” Rucinski Supp. Rep. at 7-8. Moreover, “domains can change ownership over time.” *Id.* at 9. Thus, the information that Dietrich looked up in December 2018 could not establish “the ownership of this domain two and a half years earlier” in May 2016. *Id.*

video payload could be extracted and played. *See id.* at 23, 64, 82 (Rucinski), 111-12 (Dietrich).¹⁷ They also agreed that the Channel One PCAP was manually saved onto the Firm Laptop. *See id.* at 30 (Rucinski), 120-22 (Dietrich). Indeed, Dietrich testified affirmatively that it was Vidulich who saved the Channel One PCAP – explaining that when a user exits the Wireshark program it “ask[s] you if you want to save this stream or . . . cancel it.” *Id.* at 121-22. Moreover, both experts testified, without hesitation, that packets 72 and 73 represented a failed DNS query – *not* a video transmission – and that “freetvstat.infomir.com.ua” was *not* the source of any of the video content that Vidulich viewed through the Channel One PCAP. *Id.* at 45, 65 (Rucinski), 114-17 (Dietrich).

On direct examination, Dietrich reconfirmed that the source of the streaming video viewed by Vidulich, which begins at packet 376 of the Channel One PCAP, was “streamer2de.allfreetv.net,” at the IP address 37.58.59.43. Hr’g Tr. at 87-93. He then made another effort to explain – based in part on research he had recently conducted on third-party websites¹⁸ – why he believed that “allfreetv.net” was associated with or controlled by defendant Infomir. *Id.* at 97-105. The purpose of this testimony, according to plaintiffs’ counsel, was to show that Infomir could have arrived at the same conclusion based on the Channel One XPS, and therefore was not prejudiced by not having the Channel One PCAP. Hr’g Tr. at 88, 100.¹⁹

¹⁷ At the request of attorney Dowd, during cross-examination, Rucinski demonstrated this point by playing that video content for the Court from the Channel One PCAP. Hr’g Tr. at 60-61.

¹⁸ Dietrich used “ripe.net” which he described as “an organization that is responsible for the distribution of IP address in Europe,” Hr’g Tr. at 96, and “domaintools.com,” which is “a very powerful tool which allows us to find an owner of the domain.” *Id.* at 99.

¹⁹ The Channel One XPS was first produced on June 22, 2018 – more than two years after plaintiffs filed the Vidulich Affidavit. Moreover, as noted above, plaintiffs insisted until October 5, 2018, that the Channel One XPS was created during an “unrelated preliminary investigation” and was “irrelevant” to the accuracy of the Vidulich Affidavit.

On cross-examination, Dietrich was asked whether he ever told Dunnington that the Vidulich Affidavit was inaccurate. He replied:

A. I will correct him, yes.

Q. When will you do that?

A. If I would see the affidavit, I will correct him about how the set top box communicate[s] with the server and where the video is coming from.

Q. You will do that?

A. Yes, I will.

Id. at 114-15. Dietrich explained that he first saw the Vidulich Affidavit two or three years after it was filed, “probably in January, a couple of months ago.” *Id.* at 113, 115. Before that, although he was “in communication” with plaintiffs’ attorneys, they spoke about “other issues.” *Id.* at 115.²⁰

III. LEGAL STANDARDS

A magistrate judge has broad authority to impose discovery sanctions. Orders imposing such sanctions “are ordinarily considered non-dispositive, and therefore fall within the grant of [Fed. R. Civ. P.] 72(a), ‘unless the sanction employed disposes of a claim.’” *Joint Stock Co.*

²⁰ On cross-examination, Dietrich testified that he was “connected” to Vidulich’s computer via Skype and TeamViewer on May 24, 2016 – the day the Wireshark capture was performed – and that he “explained to [Vidulich] how to start Wireshark.” Hr’g Tr. at 118. Attorney Dowd then conducted a brief redirect examination devoted entirely to other issues. *Id.* at 118-20. Seeking clarification on the TeamViewer issue, the Court asked again when Dietrich was “having this Skype and TeamViewer session.” *Id.* at 121. Dietrich replied, “[o]n the 24th of May,” meaning that he was “present in Mr. Vidulich’s computer when that PCAP was created.” *Id.* At that point, attorney Dowd sought leave to recall Dietrich and “treat the witness as hostile.” *Id.* at 124. Counsel explained that Dietrich must have been confused, because his testimony was inconsistent with his expert declaration – which stated that the Skype/TeamViewer session occurred on May 19, not May 24, 2016 – and with certain related documentary evidence. *Id.*; *see also id.* at 125 (Dowd, arguing that he should be permitted “to clean up what is damaging testimony from friendly fire”). I denied the motion. *Id.* at 128-29. As discussed in more detail below, however, I do not rely upon that portion of Dietrich’s testimony in this Opinion and Order.

Channel One Russia Worldwide v. Infomir LLC, 2017 WL 3671036, at *16 (S.D.N.Y. July 18, 2017) (quoting *Seena Int’l Inc. v. One Step Up, Ltd.*, 2016 WL 2865350, at *10 (S.D.N.Y. May 11, 2016)). This rule extends to orders precluding the introduction of specified evidence, which are “properly characterized as non-dispositive . . . [a]s long as the order does not wholly dispose of a party’s claim or defense.” *Seena Int’l Inc.*, 2016 WL 2865350, at *10 (citing, *inter alia*, *Update Art, Inc. v. Modiin Publ’g, Ltd.*, 843 F.2d 67, 71 (2d Cir. 1988)).

A. Rule 37(b)

Where, as here, sanctions are sought because a party has “fail[ed] to obey an order to provide or permit discovery,” but no ESI has been “lost,” the motion is ordinarily analyzed under Fed. R. Civ. P. 37(b)(2)(A), which permits the court to “issue further just orders,” including:

- (i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;
- (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;
- (iii) striking pleadings in whole or in part;
- (iv) staying further proceedings until the order is obeyed;
- (v) dismissing the action or proceeding in whole or in part;
- (vi) rendering a default judgment against the disobedient party; or
- (vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

In addition, the court must order the disobedient party to pay the “reasonable expenses, including attorney’s fees” incurred by the moving party, “unless the failure was substantially justified or other circumstances make an award of expenses unjust.” Fed. R. Civ. P. 37(b)(2)(C).

The only predicates to the imposition of sanctions under Rule 37(b) are a “court order directing compliance with discovery requests” and “non-compliance with that order.” *Shanghai Weiyi Int’l Trade Co. v. Focus 2000 Corp.*, 2017 WL 2840279, at *9 (S.D.N.Y. June 27, 2017). Rule 37(b) applies “notwithstanding a lack of willfulness or bad faith,” although such factors may be “relevant . . . to the sanction to be imposed for the failure.” *Oz v. Lorowitz*, 2011 WL 803077, at *2 (S.D.N.Y. Mar. 7, 2011) (quoting *Auscape Int’l v. Nat’l Geographic Soc’y*, 2003 WL 134989 at *4 (S.D.N.Y. Jan. 17, 2003)). Where, as here, ESI is “untimely produced,” a showing of “ordinary negligence will satisfy the state-of-mind requirement” under Rule 37(b). *Kortright Capital Partners LP v. Investcorp Inv. Advisers Ltd.*, 330 F.R.D. 134, 138 (S.D.N.Y. 2019) (citing *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 113 (2d Cir. 2002)); accord *In re Sept. 11th Liab. Ins. Coverage Cases*, 243 F.R.D. 114, 125 (S.D.N.Y. 2007).

Similarly, although prejudice to the moving party “may be a significant consideration” in selecting the appropriate remedy, it is not a “prerequisite” to the imposition of Rule 37(b) sanctions. *Royal Park Invs. SA/NV v. U.S. Bank Nat’l Ass’n*, 319 F.R.D. 122, 126 (S.D.N.Y. 2016); see also *Valentini v. Citicorp Fin. Servs. Corp.*, 589 F. App’x 1, 2 n.3 (2d Cir. 2014) (“an imposition of discovery sanctions requires neither a finding of bad faith nor a finding of prejudice.”); *S. New England Tel. Co. v. Glob. NAPs Inc.*, 624 F.3d 123, 148-49 (2d Cir. 2010) (“[W]e, along with the Supreme Court, have consistently rejected the ‘no harm, no foul’ standard for evaluating discovery sanctions.”).²¹

²¹ Rule 37(e), which governs sanctions for the spoliation of ESI, requires a “finding of prejudice to another party from loss of the information.” Fed. R. Civ. P. 37(e)(1). In addition, certain severe sanctions, including dismissals and default judgments, require a “finding that the [spoliating] party acted with the intent to deprive another party of the information’s use in the litigation.” Fed. R. Civ. P. 37(e)(2). However, as Judge Pauley explained in *Kortright*, “Rule 37(e) applies only when

B. Inherent Authority

“Even in the absence of a discovery order, a court may impose sanctions on a party for misconduct in discovery under its inherent power to manage its own affairs.” *Residential Funding Corp.*, 306 F.3d at 106-07. Courts frequently rely on their inherent power to sanction a party or attorney who “has made a false statement to the court and has done so in bad faith,” *S.E.C. v. Smith*, 710 F.3d 87, 97 (2d Cir. 2013), including false statements about discovery compliance. For example, in *Metro. Opera Ass’n, Inc. v. Local 100, Hotel Emps. & Rest. Emps. Int’l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003), *adhered to on reconsideration*, 2004 WL 1943099 (S.D.N.Y. Aug. 27, 2004), Judge Preska entered an adverse liability judgment, as well as monetary sanctions, where defendants made a series of false statements about “simple but material matters,” including “falsely denying [the] existence” of certain documents called for by plaintiff’s discovery requests, *id.* at 225, and where their attorneys responded to the Met’s complaints of inadequate production with “continuing representations of full compliance” that were “so lacking in a reasonable basis as to rise to the level of bad faith.” *Id.* at 224. *See also DeCastro v. Kavadia*, 309 F.R.D. 167, 184-85 (S.D.N.Y. 2015) (sanctioning attorney who “made multiple incomplete or misleading submissions

ESI ‘that should have been preserved’ is ‘lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery.’” 330 F.R.D. at 138 (quoting Fed. R. Civ. P. 37(e)). As plaintiffs acknowledge, Infomir’s motion “contains no allegation that evidence was destroyed.” Pl. Opp. Mem. at 3; *see also* Infomir Reply Mem. dated Jan. 10, 2019 (Dkt. No. 718), at 12 (“Rule 37(e) does not apply, because the PCAP was not lost or spoliated”). Where, as here, the evidence at issue was “not lost, but merely untimely produced,” the motion is governed by Rule 37(b) and “a showing of ordinary negligence will satisfy the state-of-mind requirement.” *Kortright*, 330 F.R.D. at 138 (striking portions of trial testimony concerning an investment committee meeting, and imposing monetary sanctions, where defendant failed to timely produce the minutes of the meeting).

to this Court” about his client’s discovery compliance, and then failed to correct them, “even after the inconsistencies and apparent errors in his submissions were drawn to his attention”).

IV. DISCUSSION

A. Plaintiffs’ Procedural Arguments Fail

Plaintiffs contend that Infomir’s motion is procedurally deficient under Local Civil Rule 37.1, because it did not “specify and quote or set forth verbatim in the motion papers each discovery request and response to which the motion or application is addressed.” Pl. Opp. Mem. at 15. To quote the rule, however, is to demonstrate its inapplicability here. Infomir is not moving to compel or for a protective order; consequently, the motion is not “addressed” to the parties’ original “discovery request[s] and response[s].” Rather, Infomir asserts that plaintiffs have violated a series of discovery *orders* that were previously issued by this Court. Those orders are adequately identified in Infomir’s papers. *See* Infomir Moving Mem. at 5, 6, 7.

Plaintiffs’ related claim – that their “due process rights” were violated because Infomir “promise[d]” to seek spoliation sanctions pursuant to Rule 37(e) but instead sought sanctions for failure to comply with prior discovery orders pursuant to Rule 37(b), *see* Pl. Opp. Mem. at 3, 15 – is equally meritless. Plaintiffs can hardly complain that Infomir dropped its spoliation allegations – as plaintiffs demanded – after the Channel One PCAP surfaced. Nor can they blame Infomir for the “moving target” that they themselves presented by repeatedly denying that they saved any Wireshark data, only to admit, months later, that such data existed but was “misplaced.” Pl. Opp. Mem. at 20. Infomir’s moving papers gave plaintiffs clear “notice of the sanctionable conduct,” *Mitchell v. Lyons Prof’l Servs., Inc.*, 708 F.3d 463, 467 (2d Cir. 2013), and this Court gave them

ample “opportunity to be heard,” *id.*, both in writing and at the February 6, 2019 hearing. Plaintiffs therefore have no grounds to complain about the “procedural safeguards afforded.” *Id.*²²

B. Plaintiffs Should Have Produced the Channel One PCAP Without Waiting for a Court Order

Rule 26(a)(1) requires that each party, “without awaiting a discovery request,” provide each other party with certain automatic disclosures, including “a copy – or a description by category and location – of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment.” Fed. R. Civ. P. 26(a)(1)(A)(ii). Rule 26(e) requires the disclosing party to supplement any “incomplete” disclosure in a timely manner. Fed. R. Civ. P. 26(e)(1)(A). The Channel One PCAP falls within the ambit of the automatic disclosure rules because it is the best evidence of the investigation described in the Vidulich Affidavit, which plaintiffs attach to their First Amended Complaint and rely on to “detail[] Defendant Infomir’s unlawful conduct.” FAC ¶ 197. Thus, plaintiffs violated Rule 26(a)(1)(A) by failing to produce the Channel One PCAP with their initial disclosures on May 3, 2017, or as soon thereafter as they recognized that those initial disclosures were incomplete.

²² Plaintiffs devote a substantial portion of their brief to the argument that they cannot be liable for sanctions pursuant to Rule 37(e) because “the PCAP *was not* destroyed,” but merely “misplaced.” Pl. Opp. Mem. at 20 (emphasis in the original); *see also* Blaustein Dec. ¶¶ 8, 56, 58. However, as noted above, Infomir’s motion does not accuse plaintiffs of spoliation, and does not seek sanctions under Rule 37(e) – a point that plaintiffs acknowledge elsewhere in their brief, *see* Pl. Opp. Mem. at 3, and that Infomir reiterates in its reply brief. *See* Infomir Reply Mem. at 12. Thus, Infomir did not misdirect plaintiffs in any way as to the authority on which they rely or the grounds for the sanctions they seek.

Plaintiffs argue that they had no obligation to produce the ESI underlying the Vidulich Affidavit because it “does not profess to be an expert report, nor relies on a PCAP file.” Pl. Opp. Mem. at 6. Plaintiffs are doubly wrong. First, the Vidulich Affidavit very much “relies” on the PCAP file. The attached screenshots show that the Channel One PCAP was open when they were made. That is because – as all parties now agree – Vidulich was viewing the Channel One PCAP (not the “active” stream captured three days earlier) when he made those screenshots, each of which is, essentially, a still picture of a very small portion of the Channel One PCAP.

Second, plaintiffs’ obligations under Rule 26(a)(1)(A)(ii) are not measured by what they chose to attach to the Vidulich Affidavit. The rule requires early disclosure of all documents, including ESI, that a party “may use to support its claims or defenses.” In the FAC, and in both of their summary judgment motions, plaintiffs implicitly asserted that the Channel One PCAP – specifically, packets 72 and 73 – shows that Infomir was unlawfully streaming a pirated version of their programming over the Internet. More recently, in the Dietrich Declaration and at the sanctions hearing, plaintiffs expressly asserted that a different portion of the Channel One PCAP – specifically, packet 376 (which was *not* discussed by Vidulich and *not* shown in the Channel One Screenshots) – supports the same claim. Indeed, according to attorney Dowd, “the PCAP file is really one of the best pieces of evidence in our case.” Hr’g Tr. at 6. If so, it should have been produced pursuant to Rule 26(a)(1)(A)(ii).

Even assuming, *arguendo*, that plaintiffs had so little understanding of the Channel One PCAP in May 2017 that they did not then realize it could support their claims, they should have produced it in response to Infomir’s initial document demands, which requested “[a]ny and all documents relating to any inspection, test or examination of any device alleged to be originating

from or the responsibility of Infomir.” Infomir Ltr. dated Feb. 6, 2018, Ex. A (Dkt. No. 516-1), at 23 (Doc. Req. No. 56). On June 7, 2017, in response to that request, plaintiffs agreed to “produce non-privileged responsive documents to the extent they exist.” *Id.* at 24. Having so responded, plaintiffs were required to produce – or log as privileged – all responsive documents. *See* Fed. R. Civ. P. 34(b)(2)(C), advisory committee note to 2015 amendment (“an objection to a Rule 34 request must state whether anything is being withheld on the basis of the objection”).

The Channel One PCAP was a “non-privileged responsive document.” The ESI underlying the Wireshark Investigation lost any work-product protection it originally enjoyed when plaintiffs filed the Vidulich Affidavit. *See United States v. Nobles*, 422 U.S. 225, 239-40 (1975) (“Respondent, by electing to present the investigator as a witness, waived the privilege with respect to matters covered in his testimony.”) The same is true for the Channel One XPS. Consequently, plaintiffs should have produced both the PCAP file and the XPS file in June 2017. They did not. Nor did they log them as privileged – which at least would have alerted Infomir to their existence and permitted it to seek judicial assistance in obtaining them. Instead, in violation of Rule 34(b), plaintiffs ignored the responsive documents entirely.

It is perhaps worth noting here – before reaching the even more pointed language contained in the Court’s later discovery orders – that plaintiffs cannot excuse their discovery failures on the ground that Infomir did not request “a .pcap specifically.” Blaustein Decl. ¶ 16; *see also* Pl. Opp. Mem. at 9 (“As discovery progressed, Infomir . . . refused to identify any specific evidence, including ESI and to be clear, the PCAP, that it claimed Broadcasters did not produce as required.”). When asked for letters or memoranda, a party cannot withhold documents stored as Microsoft Word files because the requesting party failed to ask for “a .docx specifically.”

Similarly, when asked for communications, a party cannot withhold Outlook email files on the ground that the requesting party failed to ask for “.pst specifically.” See *Star Direct Telecom, Inc. v. Glob. Crossing Bandwidth, Inc.*, 272 F.R.D. 350, 359 (W.D.N.Y. 2011) (rejecting defendant’s contention “that it was not required to produce emails because plaintiffs’ document requests did not specify the form in which the electronically stored information was to be produced”); Fed. R. Civ. P. 34(a)(1)(A) (Rule 34 requests reach ESI “stored in any medium from which information can be obtained”). By the same token, when asked for documents underlying an investigation conducted in Wireshark, a party cannot withhold ESI stored in Wireshark’s native format²³ because the requesting party failed to ask for “.pcap specifically.”

The motion now before the Court does not seek sanctions under Rule 37(c) for plaintiffs’ initial failure to produce the Chanel One PCAP in 2017. Nor, of course, does it seek another Rule 37(a) order compelling disclosure of that file. Rather, Infomir requests a Rule 37(b) order sanctioning plaintiffs for violating Rule 37(a) orders issued in 2018. However, when deciding a Rule 37(b) motion, “[t]he district court is free to consider ‘the full record in the case in order to select the appropriate sanction.’” *S. New England Tel. Co.*, 624 F.3d at 144 (quoting *Nieves v. City of New York*, 208 F.R.D. 531, 535 (S.D.N.Y. 2002)). Consequently, in determining the degree of plaintiffs’ fault and selecting appropriate sanctions, I need not ignore the fact that their obligation to produce the PCAP file arose well before I issued the orders at issue on the instant motion.

²³ The parties are agreed that “the native file format for a Wireshark capture is ‘.pcap.’” 10/12/18 Vidulich Aff. ¶ 8; see also Pl. Opp. Mem. at 12; Blaustein Decl. (Dkt. No. 711) ¶ 53; Rucinski Rep. at 9, 12.

C. Plaintiffs Violated Two Court Orders

Infomir claims that plaintiffs' failure to turn over the Channel One PCAP violated three separate discovery orders: the 2/13/18 Order, the 4/25/18 Order, and the 7/3/18 Order. Plaintiffs counter that "those orders do not specifically compel the production of a PCAP, which . . . Infomir did not request until September of 2018." Pl. Opp. Mem. at 1. Plaintiffs are correct that the 2/13/18 Order did not require them to produce the Channel One PCAP. However, the 4/25/18 Order and the 7/3/18 Order did. Moreover, they did so in terms that were abundantly clear for attorneys of ordinary intelligence and minimal technological competence.

1. The 2/13/18 Order

As noted above, the Channel One PCAP was responsive to Infomir's document request No. 56, seeking "[a]ny and all documents relating to any inspection, test or examination of any device alleged to be originating from or the responsibility of Infomir." However, at the February 9, 2018 discovery conference, when Infomir asked for an order compelling plaintiffs to supplement their response to No. 56, it expressly limited the scope of the proposed order to inspections, tests, or examinations conducted by "plaintiffs, not their attorneys." 2/9/18 Conf. Tr. at 121:15-19. Consequently, I directed plaintiffs, on the record, to provide a supplemental response to No. 56 "with respect to any hardware testing conducted not by counsel or by an expert under counsel's direction but by the client." *Id.* at 121:21-24. The 2/13/18 Order, which instructed plaintiffs to supplement their response to No. 56 "as directed on the record at the February 9 discovery conference," *id.* ¶ 7, incorporated the same limits. Since the Wireshark Investigation was conducted by Dunnington, rather than by plaintiffs themselves (which Infomir knew during the February 9 conference), I cannot conclude that the 2/13/18 Order, read fairly, required plaintiffs to produce the Channel One PCAP.

2. The 4/25/18 Order

The 4/25/18 Order, by way of contrast, expressly required plaintiffs to produce:

any additional documents in their possession, custody, or control (beyond those attached as exhibits to the witness's various declarations) constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities.

This order arose after plaintiffs filed their second summary judgment motion, which relied on the Vidulich Affidavit to establish the “undisputed fact” that “[t]he video stream of Channel One Programming originated from the domain `freetvstat.iptv.infomir.com.ua`.” Pl. Rule 56.1 St. dated March 23, 2018 (Dkt. No. 551), ¶ 146; *see also* Pl. Mem. dated March 23, 2018, at 6 (plaintiffs “tracked U.S. video streams of pirated Channel One programming viewed on Infomir STBs to an Infomir affiliated server, `freetvstat.iptv.infomir.com.ua`, located in Ukraine”). Given the significance of these factual assertions to plaintiffs’ motion, Infomir noticed the Vidulich deposition and sought additional ESI, arguing that plaintiffs should be required to disclose “complete” information regarding the Wireshark Investigation, including “the electronically stored data from the ‘network protocol analyzer’ referenced in Mr. Vidulich’s affidavits.” Joint Ltr. dated Apr. 16, 2018, at 4; *see also* 4/19/2018 Conf. Tr. at 97:2-5 (asking for the “data file that was generated when Mr. Vidulich used what you call a network analyzing program”); *id.* at 97:7-10 (“we’re entitled to see the full data file”); *id.* at 98:3-4 (“[w]e want to see the full data set”).

Plaintiffs opposed the request – arguing that previously undisclosed Wireshark ESI was subject to the work product doctrine, *see* Joint Ltr. dated Apr. 16, 2018, at 5 – but never suggested that they did not understand the request, nor that they could not extract the requested files. To the contrary: attorney Blaustein assured the Court that Dunnington had “an in house computer person,

a network specialist,” whom he would “ask about identifying the specific data” or, if necessary, Dunnington would “go to an outside source.” 4/19/2018 Conf. Tr. at 99:20-22, 100:6-9.

It is true, as plaintiffs point out, that the 4/25/18 Order did not use the word “PCAP.” *See* Pl. Opp. Mem. at 1, 2, 3, 10, 17, 18; Blaustein Decl. ¶ 34. It did not have to. The Court directed plaintiffs to produce all remaining documents “constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities.” 4/25/18 Order at 5. There can be no genuine dispute but that the Channel One PCAP falls squarely within that mandate. Nor can Dunnington credibly contend – particularly in light of the discussion at the April 19 conference – that it did not understand that the 4/25/18 Order required the production of the “full data file” generated by the Wireshark Investigation. *See* 4/19/2018 Conf. Tr. at 97:7-10.

The Court accepts that Wireshark is less familiar to the general public (and most lawyers) than commonly-used word processing and email programs. But it was Dunnington’s choice to use Wireshark to gather evidence concerning Infomir’s alleged streaming activities. It was therefore Dunnington’s responsibility – not Infomir’s or the Court’s – to understand the technology well enough to know where and how to preserve, locate, and produce discoverable ESI created by or saved within that program. *See* N.Y. Rules of Prof’l Conduct, R. 1.1 (“Competence”), cmt. 8 (“To maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information”). New York lawyers are “not required to stay current with every new app and every new form of technology – that would be impossible.” 1 Roy D. Simon & Nicole Hyland, *Simon’s New York Rules of Professional Conduct Annotated* § 1.1:9 (2019). But they “must understand” the technology that they “actually use[],” and “keep up with changes in that

technology.” *Id.* Dunnington “actually used” Wireshark. Moreover, the firm had a “network specialist” in house, 4/19/2018 Conf. Tr. at 99:20-22, and access to “an outside source,” *id.* at 100:6-9, later identified as the Chief Technology Officer of Kartina, who tutored Vidulich in the use of the Wireshark program. 12/20/18 Vidulich Aff. ¶ 5. On these facts, plaintiffs cannot excuse their failure to produce the Channel One PCAP by complaining that the 4/25/18 Order failed to provide its file extension.

Plaintiffs’ alternative argument – that they “fully complied” with the 4/25/18 Order by offering the Firm Laptop to Infomir for inspection, *see* Pl. Opp. Mem. at 2, 3, 4, 18; Blaustein Decl. ¶¶ 4, 8 – fares no better.²⁴ It is well-settled that a producing party cannot unilaterally shift the burden and expense of complying with its discovery obligations to its opponent by “simply dumping large quantities of unrequested materials onto the discovering party along with the items actually sought.” 8B Charles Alan Wright & Authur R. Miller, *Federal Practice and Procedure* § 2213, at 189-90 (3d ed. 2010); *see also Novak v. Yale Univ.*, 2015 WL 7313855, at *3 (D. Conn. Nov. 20, 2015) (sanctioning plaintiff pursuant to Rule 37(b) for responding to an earlier discovery order with “a ‘document dump,’ which largely left defendant with a mass of unmanageable and unusable documents”); *Levene v. City of New York*, 1999 WL 397482, at *3 (S.D.N.Y. June 15, 1999) (dismissing case pursuant to Rule 37(b) where plaintiff responded to the court’s discovery orders by “dump[ing] on defendants over 10,000 pages of documents,” most of which were not responsive to those orders), *aff’d*, 216 F.3d 1072 (2d Cir. 2000). Such tactics improperly shift the

²⁴ Plaintiffs assert that when they first offered the Firm Laptop for inspection it was “pristine,” Pl. Opp. Mem. at 3, 18, presumably meaning that Vidulich had not yet removed the Channel One PCAP from that laptop.

cost of compliance from the recalcitrant party – whose conduct necessitated the order – to the party for whose benefit it was issued.

In this case, the ESI that I ordered plaintiffs to produce was created, saved, and stored by their own counsel, using a sophisticated software program of counsel’s choosing. Moreover, that ESI resided on a Dunnington laptop, which, according to attorney Blaustein, “was used for more than just this purpose” and contained “an internal drive that presumably has client information for every client that we serve.” 4/19/18 Conf. Tr. at 99:5-15. Plaintiffs’ offer to “dump” the laptop on Infomir – which, as they knew, would require its opponent to “pay for a forensic evaluation,” Blaustein Decl. ¶ 59 – was not an acceptable substitute for locating, copying, and turning over the Wireshark data contained on that laptop, which is what this Court directed them to do.²⁵

These harms are not merely theoretical. When Infomir ultimately agreed to examine the Firm Laptop, it was required to retain its own computer experts, likely at considerable expense. Additionally, the presence of so much irrelevant (and potentially privileged) information on the laptop required Infomir to agree to a complex procedure to ensure that it did not inadvertently gain

²⁵ In their motion papers, plaintiffs were indignant that Infomir balked, for a time, at being asked to shoulder the burden and expense of the forensic exam. *See* Blaustein Decl. ¶¶ 4, 8, 33, 59 (complaining that Infomir “insisted” or “demanded” that Dunnington do the work to locate and produce any relevant ESI on the Firm Laptop). Plaintiffs seem to have lost sight of the fact that this was, in fact, their responsibility. *See, e.g., Metro. Opera Ass’n*, 212 F.R.D. at 221 (quoting *Tarlton v. Cumberland Cty. Corr. Facility*, 192 F.R.D. 165, 170 (D.N.J. 2000)) (“Under the federal rules, the burden does not fall on plaintiff to learn whether, how and where defendant keeps relevant documents.”).

access to confidential materials pertaining to other Dunnington clients.²⁶ These procedures, in turn, increased Infomir's costs and further delayed discovery, including the Vidulich deposition.²⁷

If Dunnington lacked the “in house” expertise to discharge its obligations under the 4/25/18 Order, it should have made arrangements with its “outside source” to handle its responsive ESI competently. *See, e.g., Pugh-Ouza v. SpringHill Suites*, 2019 WL 3557794, at *10 (S.D.N.Y. July 9, 2019) (requiring defendants to “secure the assistance of a forensic expert to determine whether the remaining audio may be recovered from [an individual defendant's] phone”), *report and recommendation adopted*, 2019 WL 3554014 (S.D.N.Y. Aug. 5, 2019); *Novak*, 2015 WL 7313855, at *3 (noting that plaintiff could have timely complied with the court's discovery order “via consultation with an electronic discovery or information technology consultant”). Instead, counsel delegated their responsibilities to a paralegal with “no specialized technical knowledge” or relevant technical background (beyond his training session with Dietrich). Vidulich Aff. ¶ 2; 9/21/18 Vidulich Aff. ¶ 2; 10/12/18 Vidulich Aff. ¶ 2; 12/20/18 Vidulich Aff. ¶ 2.

This proved to be a serious mistake. Although Vidulich understood the 4/25/18 Order well enough to look for “Wireshark data” on the Firm Laptop, 10/18/18 Vidulich Aff. ¶ 4, his handling of that data was – at best – incompetent. He located the Channel One PCAP and the Channel One XPS, identified them as potentially responsive to that Order, and moved them to a different

²⁶ The parties' Stipulated Order required Infomir's experts at Stroz Friedberg to mirror the Firm Laptop's hard drive, return the original, search the mirrored copy for Wireshark-related files, “generate a list of files and data responsive to the search,” submit the list to Dunnington for review, and wait five business days for Dunnington to review the list for privilege concerns. Only then, and only if no privilege concerns were raised, was Stroz Friedberg permitted to disclose the Wireshark files to Infomir. *See* Stip. Order ¶¶ 1-5.

²⁷ *See* Stip. Order ¶¶ 6-11.

computer. *Id.* ¶ 5.²⁸ In the process, however, he also removed the PCAP file from the Firm Laptop, leaving only an artifact to show that it had once existed.²⁹ Moreover, once the Wireshark files were moved, Vidulich overlooked the Channel One PCAP, which he was unable to “open,” *id.* ¶ 7, and plaintiffs produced only the Channel One XPS (which they then falsely claimed to be unrelated to the investigation described in the Vidulich Affidavit). Thereafter, insofar as the record discloses, Vidulich and his attorney supervisors made no further effort to produce the Channel One PCAP for approximately three and a half months, until after the October 5, 2018 discovery conference, *id.* ¶¶ 8-10, when Infomir’s counsel (who by then had been educated by Stroz Friedberg) provided what amounted to a PCAP tutorial.

On this record, the Court concludes, without difficulty, that plaintiffs violated the 4/25/18 Order by failing to produce the Channel One PCAP.

3. The 7/3/18 Order

The 7/3/18 Order was, if anything, even more precise. It was issued after Dunnington moved the Wireshark files from the Firm Laptop to another computer but produced only the XPS file, dated May 24, 2016. Frustrated by the lack of any comparable data evidencing what Infomir still understood to have been a May 27, 2016 Wireshark capture, and skeptical that no further files existed, Infomir asked the Court, on June 26, 2018, for an order directing plaintiffs to “produce what they have and make a representation that there’s nothing else available.” 6/26/18 Conf. Tr.

²⁸ Vidulich may have been aided in this task by the Channel One Screenshots, which did list the Channel One PCAP by name. *See* Vidulich Aff. Exs. 14, 16 (showing the open file as “Channel One Capture.pcapng”).

²⁹ *See* Pl. Ltr. dated Oct. 18, 2018, at 2; *id.* Ex. A at ECF page 2.

at 140:7-8. On July 3, 2018 – after Infomir elected to examine the Firm Laptop – the Court made plaintiffs’ obligations clear:

Infomir contends that plaintiffs have not yet fully complied with several provisions of the April 25 Order, including ¶ 4, which required them to produce “any additional documents . . . constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities.” *For example, according to Infomir, plaintiffs have not produced any data from “any ‘network protocol analyzer,’ ‘Wireshark,’ or similar investigative process” employed by Vidulich on April [sic] 27, 2016.* This data is significant, plaintiffs argue, because in ¶ 30 of his June 24, 2016 affidavit Vidulich swore that as a result of the investigations performed that day, using a network protocol analyzer, he learned that Infomir was involved in “content distribution activity.” Among other things, Vidulich attested, he learned that the set-top box through which he viewed plaintiff’s Channel One broadcast connected to “freetvstat.iptv.infomir.com.ua,” with an IP address located within the United States. Plaintiffs, for their part, represent that they have produced all of the data they were able to extract from Mr. Vidulich’s laptop. *No later than **July 10, 2018**, plaintiffs shall conduct a further search of their records, including ESI, and shall produce any additional documents constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities.*

7/3/18 Order ¶ 7 (record citations omitted; additional emphasis added). For avoidance of doubt, the Court added that Infomir’s decision to examine the Firm Laptop “does not relieve plaintiffs of their obligation, set forth above, to produce any additional documents constituting or recording the information and data that Vidulich acquired as a result of his investigatory activities no later than **July 10, 2018.**” *Id.* ¶ 8 (emphasis in the original).

Once again, I conclude that the Court’s order was “clearly articulated,” *Daval Steel Prods., a Div. of Francosteel Corp. v. M/V Fakredine*, 951 F.2d 1358, 1363 (2d Cir. 1991), and required “specified discovery,” *id.*, but that plaintiffs failed to comply. The 7/3/18 Order required production of the Wireshark data underlying the Vidulich Affidavit by July 10, 2018, and specified that the turnover of the laptop did not satisfy that obligation. Nonetheless, plaintiffs failed to produce the PCAP file for another three months. In the meantime, Infomir attempted to take

Vidulich’s deposition without the underlying data, only to hear him repeat statements that all parties now understand to have been untrue, including that the Wireshark capture occurred on May 27, 2016; that he was “viewing Channel One” on an “active” stream when he created the Channel One Screenshots; that he did not “save the Wireshark capture data” except “[a]s a screen shot”; and that he “didn’t delete anything” from the Firm Laptop. Vidulich Dep. Tr. at 28:4-19, 32:1-25, 46:7-15, 73:16, 98:13-99:4, 99:17-21.

Plaintiffs’ defense – that they did not understand what was required of them because the 7/3/18 Order did not use the term “PCAP” – is even less convincing in the context of the 7/3/18 Order. Not only are the terms of the order clear; by the time it was issued, Vidulich had already looked for “Wireshark data” on the Firm Laptop, found the Channel One PCAP, and moved it to another computer for production purposes. 10/18/18 Vidulich Aff. ¶¶ 4-10. Thus, even if I credit plaintiffs’ contention that the PCAP file was “inadvertently” not produced in June 2018, Pl. Opp. Mem. at 2, I cannot accept counsel’s representation that no one at Dunnington knew it “existed,” Blaustein Aff. ¶ 4, until the following October. Moreover, Dunnington’s technological incompetence (including Vidulich’s asserted inability to open the Channel One PCAP) has no bearing on the clarity of the order that plaintiffs violated as a result of that incompetence.

D. Plaintiffs Made a Series of False Statements in Bad Faith

Plaintiffs did not merely fail to produce the Channel One PCAP in a timely manner. Through their investigator and their counsel, they made numerous false statements of fact (many under oath) about the Wireshark Investigation, the ESI evidencing that investigation, and their discovery compliance, including:

- (1) That the Wireshark capture occurred on May 27, 2016, *see* Vidulich Aff. ¶¶ 18-23; Vidulich Dep. Tr. at 32:1-25; 9/21/18 Vidulich Aff. ¶ 11; Pl. Ltr. dated Sept. 21, 2018, at 3, when in fact it occurred three days earlier;
- (2) That Vidulich was watching an “active” Channel One stream on May 27, 2016, when he took the Channel One Screenshots, *see* Vidulich Aff. ¶¶ 24, 26, Vidulich Dep. Tr. at 32:1-25, when in fact he was watching the Channel One PCAP;
- (3) That the Channel One XPS, dated May 24, 2016, reflected an “unrelated preliminary” investigation that Vidulich did not “reference” in his original affidavit and that plaintiffs never “relied on,” *see* 9/21/18 Vidulich Aff. ¶¶ 14-17, 19; Pl. Ltr. dated Sept. 21, 2018, at 3, when in fact that XPS file documented the same May 24 Wireshark capture reflected in the Channel One Screenshots and the (as yet unproduced) Channel One PCAP;
- (4) That no Wireshark data was saved (other than the Channel One Screenshots), and that Vidulich did not know how to save such data or what a PCAP file was, *see* Vidulich Dep. Tr. at 99:3-4, 17-22; 9/21/18 Vidulich Aff. ¶¶ 6, 13, when in fact he manually saved all of the data captured by Wireshark on May 24 to the Firm Laptop, in native PCAP format, and named the file “Channel One Capture.pcapng”;³⁰ and
- (5) That Dunnington had produced “everything” in connection with the Wireshark Investigation, including “[a]ll the documents [Vidulich] created” and the “one file” they found on the Firm Laptop, *see, e.g.*, 6/26/18 Conf. Tr. at 137:8-9, 12-13, 138:23-139:3, 139:22-23; Pl. Ltr. dated Sept. 21, 2018, at 3; 9/21/18 Vidulich Aff. ¶¶ 6-7, 11; 10/5/18 Tr. at 67:6-15, when in fact a Dunnington employee moved the Channel One PCAP from the Firm Laptop to another firm computer on June 22, 2018, and left it there, unproduced, while counsel vehemently denied that it existed.

These statements, taken together, formed a near-constant stream of factual misdirection that significantly delayed – and nearly derailed – Infomir’s efforts to obtain highly probative ESI that plaintiffs were twice ordered to produce. Moreover, most of the misstatements related to “simple but material factual matters,” *Metro. Opera Ass’n*, 212 F.R.D. at 225, that required no “specialized technical knowledge” to report accurately (or to correct if initially misstated), such as when the Wireshark capture took place and whether Vidulich was watching the Channel One

³⁰ In addition, either Vidulich or someone else at Dunnington saved a portion of that data in the form of the Channel One XPS.

stream “live,” as opposed to re-running an earlier Wireshark capture, when he took the Channel One Screenshots. Similarly, plaintiffs’ lawyers and investigator cannot blame their lack of computer science degrees for their response to Informir’s inquiries about the Channel One XPS, which was dated May 24 rather than May 27, 2016. Rather than make a reasonable inquiry into the reason for the discrepancy, Dunnington went on the offensive, inventing an “unrelated preliminary investigation” that Vidulich supposedly conducted on May 24 but never described in his original affidavit. 9/21/18 Vidulich Aff. ¶¶ 14-17; Pl. Ltr. dated Sept. 21, 2018, at 3. This invention, in turn, allowed counsel to claim that the XPS file “has no bearing whatsoever” on plaintiffs’ allegations. 9/21/18 Vidulich Aff, ¶ 17.³¹ Even if not perjurious, these statements were made so cavalierly, with so little regard for counsel’s duties of candor and diligence, “as to rise to the level of bad faith.” *Metro. Opera Ass’n*, 212 F.R.D. at 224; *see also DeCastro*, 309 F.R.D. at 184-85 (finding bad faith where attorney “made multiple incomplete or misleading submissions” about his client’s discovery compliance and failed to correct them even when alerted to their “inconsistencies and apparent errors”).

As for the Channel One PCAP: someone manually saved that file to the Firm Laptop and named it “Channel One Capture.pcapng.” According to Dietrich, that someone was Vidulich. *See Hr’g Tr.* at 121-22. Vidulich himself has been oddly silent on this point since the Channel One PCAP was produced. The affidavits he filed on and after October 12, 2018 do not explain, discuss, or even mention his earlier testimony that there never was any PCAP file. *See* 9/21/18 Vidulich

³¹ By the time of the sanctions hearing, plaintiffs were taking a very different position: that the Channel One XPS contained almost all of the same information (albeit in a less convenient format) as the Channel One PCAP, including the information necessary for Infomir to determine where the Channel One video stream was coming from, and therefore that Infomir was not prejudiced by the delay in producing the PCAP file. *See, e.g., Hr’g Tr.* at 88.

Aff. ¶ 6 (“the Wireshark data . . . was not saved”); *id.* ¶ 21 (the Wireshark data “was never saved, and therefore could not have been produced”). Nor has Vidulich explained or clarified, in any way, his prior testimony that he “did not even know how to properly save Wireshark data, let alone what the native format of Wireshark data is.” *Id.* ¶ 21.

On this record, I have little choice but to conclude that Vidulich’s misstatements were either intentional or – at best – the product of an exceptionally faulty memory, which neither he nor his supervisors made any effort to jog (such as, for example, by asking Dietrich to remind him what file format to look for or help him open the one he moved from the Firm Laptop to his desktop computer on June 22, 2018).³² By the same token, it was – at best – grossly negligent for the Dunnington attorneys to rely, “apparently without any investigation, on [Vidulich’s] dubious assertions,” including his assertion that he never saved any PCAP file, “and offer[] them unhesitatingly to this Court.” *DeCastro*, 309 F.R.D. at 185.

Indeed, unlike the sanctioned attorney in *DeCastro* (whose misconduct consisted largely of failing to rein in a client who was “deliberately engaged” in discovery misconduct, 309 F.R.D. at 184), plaintiffs’ counsel exercised considerable control over Vidulich, who was – quite literally – on their payroll. Dunnington assigned him to conduct the Wireshark Investigation, furnished the

³² There is, of course, another possibility: that Dietrich, or someone else at Kartina, had remote control of the Firm Laptop on May 24, 2016, and used that control to save the PCAP file. The only evidence for this theory, however, is Dietrich’s testimony at the sanctions hearing, which – although clear – was inconsistent with the remainder of the record, including a photograph, offered at the hearing, depicting a TeamViewer session on May 19. Moreover, after the PCAP file was produced, Vidulich admitted, under oath, that on May 27 “I took screenshots of the Wireshark data *that I had previously captured* in order to attach it to my affidavit.” 12/20/18 Vidulich Aff. ¶ 7 (emphasis added). I therefore find that it was Vidulich, working under counsel’s supervision, who saved the Channel One PCAP on May 24, and that Dietrich was – as attorney Dowd suggested – mistaken as to the date of what all witnesses agree was a single TeamViewer training session.

necessary equipment, and supervised his work, which was performed in a Dunnington conference room under the eyes of the same lawyers who later told this Court, inaccurately, that no relevant ESI was saved. *See* Hr’g Tr. at 7 (Dowd) (“I was standing in the room as he did it.”).

Of course counsel knew that Vidulich lacked any relevant technical background. Rather than retain a technically competent investigator, however, plaintiffs’ attorneys appear to have made a deliberate decision to put the Wireshark investigation into the hands of a novice, which they then sought to turn to their advantage.³³ Similarly, rather than ask their “in house computer person” or an “outside source” to identify and produce the Wireshark data on the Firm Laptop, as promised, counsel delegated the task of complying with the 4/25/18 Order and the 7/3/18 Order to Vidulich. Even after Infomir told plaintiffs that a PCAP file called “Channel One Capture.pcapng” had once been saved to the laptop but was no longer there (because, plaintiffs now acknowledge, Vidulich “inadvertently” moved it), counsel left discovery compliance in Vidulich’s hands, and continued to claim that they had turned over “[e]verything that was saved or screen shot.” 10/5/18 Tr. at 67:6-15. When caught out, counsel again attempted to turn their reliance on underqualified staff to strategic advantage.³⁴

In short, plaintiffs’ counsel, like defendant’s counsel in *Metro. Opera Ass’n*, “continually professed full compliance – falsely and, as confirmed by [subsequent events], without making a

³³ *See, e.g.*, Pl. Ltr. dated Sept. 21, 2018, at 4 (arguing that plaintiffs should not be liable for spoliation because “Vidulich saved what he understood as a non-expert to be the relevant data, namely the Wireshark output, by screenshotting it”).

³⁴ *See, e.g.*, Pl. Ltr. dated Oct. 12, 2018, at 3 (arguing that plaintiffs should not be faulted for their late production of the Channel One PCAP because, “while a forensic expert employed by the FBI may be expected to understand that apcap file would be important . . . a non-expert like Mr. Vidulich investigating infringement of television channels would not”).

reasonable inquiry.” 212 F.R.D. at 222. This conduct alone “constitutes such gross negligence as to rise to intentional misconduct.” *Id.* Moreover, counsel did not merely look the other way when Vidulich made factually dubious statements to the Court. In addition to filing his affidavits (which they likely assisted in drafting), counsel amplified, repeated, and affirmatively vouched for his testimony in their own letters, affidavits, and court presentations.³⁵ I therefore conclude that plaintiffs engaged in “a pattern of behavior which could reasonably be construed as a bad faith effort to thwart [Infomir’s] discovery efforts.” *DLC Mgmt. Corp. v. Town of Hyde Park*, 163 F.3d 124, 135-36 (2d Cir. 1998) (affirming adverse inference and monetary sanctions pursuant to the court’s inherent powers where defendants belatedly produced a box of relevant documents, past the discovery cut-off, after finding it “where it had always been – in a Town Hall closet that defendants apparently had never bothered to search”).

E. Monetary Sanctions and Preclusion Are Warranted

1. Standards

“Disciplinary sanctions under Rule 37 are intended to serve three purposes. First, they ensure that a party will not benefit from its own failure to comply. Second, they are specific deterrents and seek to obtain compliance with the particular order issued. Third, they are intended to serve a general deterrent effect on the case at hand and on other litigation, provided that the party against whom they are imposed was in some sense at fault.” *S. New Eng. Tel. Co.*, 624 F.3d at 149 (quoting *Update Art, Inc.*, 843 F.2d at 71).

³⁵ See, e.g., Affidavit of Raymond J. Dowd Confirming Accuracy and Procedure of Christopher Vidulich, dated Dec. 20, 2018 (Dkt. No. 712), ¶¶ 8-10 (attesting that attorney Dowd “witnessed Mr. Vidulich using Wireshark” in May 2016 and “confirm[ing] that Mr. Vidulich’s description of his use of Wireshark to capture data from the Aura HD STB while streaming Russian language programming was accurate in his affidavit”).

District courts have “broad discretion in fashioning an appropriate sanction” for discovery violations. *Residential Funding Corp.*, 306 F.3d at 101; *see also Linde v. Arab Bank, PLC*, 706 F.3d 92, 115 (2d Cir. 2013) (“there are few bright-line rules for determining whether a sanction is proper”); *Luft v. Crown Publishers, Inc.*, 906 F.2d 862, 865 (2d Cir. 1990) (the decision to impose a particular discovery sanction “is committed to the sound discretion of the district court and may not be reversed absent an abuse of that discretion”).

The “mildest” sanction under Rule 37(b) “is an order to reimburse the opposing party for expenses caused by the failure to cooperate.” *Seena Int’l Inc.*, 2016 WL 2865350, at *11 (quoting *Cine Forty-Second St. Theatre Corp. v. Allied Artists Pictures Corp.*, 602 F.2d 1062, 1066 (2d Cir. 1979)). “Monetary sanctions are the norm, not the exception, when a party is required to engage in motion practice in order to obtain the discovery to which it is entitled.” *Id.*

“If monetary sanctions are not sufficient, more stringent orders may be issued,” including preclusion orders, adverse inference orders, and orders deeming disputed facts determined adversely to the disobedient party. *Joint Stock Co. Channel One*, 2017 WL 3671036, at *19-20 (quoting *Seena Int’l Inc.*, 2016 WL 2865350, at *12) (internal quotation marks omitted). “Such sanctions affect the merits of the litigation by placing the risk of a verdict uninformed by important facts on the party that made evidence of those facts unavailable in the discovery process.” *Hand Picked Selections, Inc. v. Handpicked Wines Int’l Pty Ltd.*, 2006 WL 1720442, at *3 (E.D.N.Y. June 22, 2006). These sanctions are particularly appropriate where the harm arising from the discovery failure is not merely “a matter of costs.” *Id.* They also serve to “enforce compliance with the discovery rules and maintain a credible deterrent to potential violators.” *Daval Steel Prods.*,

951 F.2d at 1367 (citing *Nat'l Hockey League v. Metro. Hockey Club, Inc.*, 427 U.S. 639, 643 (1976)).

In this Circuit, as noted above, “negligence is generally sufficient to establish culpability for purposes of imposing most sanctions,” *Fitzpatrick v. Am. Int’l Grp., Inc.*, 2013 WL 9948284, at *9 (S.D.N.Y. May 29, 2013) (citing *Residential Funding Corp.*, 306 F.3d at 108), including non-dispositive preclusion orders. *See, e.g., Brown v. City of New York*, 2018 WL 3193208, at *2 (E.D.N.Y. June 28, 2018) (upholding magistrate judge’s order issuing preclusion and monetary sanctions where defendants negligently failed to produce a key audio recording until after discovery closed, blaming the delay on “inadvertent clerical error”); *New York State Nat. Org. for Women v. Cuomo*, 1997 WL 671610, at *5 (S.D.N.Y. Oct. 28, 1997) (preclusion sanctions “may be imposed where the failure to meet discovery obligations is not willful, but merely negligent”).

The most “severe” measures, including terminating sanctions, are ordinarily reserved for cases involving “intentional behavior, actions taken in bad faith, or grossly negligent behavior,” *Metro. Opera Ass’n*, 212 F.R.D. at 219, including “gross professional negligence.” *See Cine Forty-Second Street Theatre Corp.*, 602 F.2d at 1068 (“where gross professional negligence has been found[,] that is, where counsel clearly should have understood his duty to the court[,] the full range of sanctions may be marshalled”); *Am. Cash Card Corp. v. AT&T Corp.*, 210 F.3d 354, 2000 WL 357670, at *5 (2d Cir. Apr. 6, 2000) (summary order) (affirming terminating sanctions and rejecting appellants’ attempt to “avoid responsibility for their failure to obey the district court’s discovery orders by shifting the blame to the incompetence of their trial counsel”). Likewise, bad faith is required “for the imposition of sanctions under the inherent power doctrine.” *DLC Mgmt. Corp.*, 163 F.3d at 136.

Any sanction imposed under Rule 37(b) must be “just,” and its severity “must be commensurate with the non-compliance.” *Joint Stock Co. Channel One*, 2017 WL 3671036, at *21 (quoting *Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 140 (2d Cir. 2007)). The sanction imposed must also “relate to the particular claim to which the discovery order was addressed.” *Seena Int’l Inc.*, 2016 WL 2865350, at *14 (quoting *Daval Steel Prods.*, 951 F.2d at 1366). Within these broad parameters, the district court’s discretion is guided by the application of four factors: “(1) the willfulness of the non-compliant party or the reason for noncompliance; (2) the efficacy of lesser sanctions; (3) the duration of the period of noncompliance; and (4) whether the non-compliant party had been warned of the consequences of noncompliance.” *S. New Eng. Tel. Co.*, 624 F.3d at 144 (quoting *Agiwal v. Mid Island Mortg. Corp.*, 555 F.3d 298, 302-03 (2d Cir. 2009)). “[T]hese factors are not exclusive, and they need not each be resolved against the party challenging the district court’s sanctions for us to conclude that those sanctions were within the court’s discretion.” *Id.*

While a court “should always seek to impose the least harsh sanction that will remedy the discovery violation and deter such conduct in the future,” *Joint Stock Co. Channel One*, 2017 WL 3671036, at *21 (quoting *Grammar v. Sharinn & Lipshie, P.C.*, 2016 WL 525478, at *3 (S.D.N.Y. Feb. 8, 2016)), it need not “exhaust possible lesser sanctions.” *Shcherbakovskiy v. Seitz*, 450 F. App’x 87, 88 (2d Cir. 2011).

2. Monetary Sanctions

Given plaintiffs’ unjustified failure to obey two clearly articulated discovery orders issued by this Court, they and their counsel must pay Infomir’s “reasonable expenses, including attorneys’ fees, caused by the failure.” Fed. R. Civ. P. Rule 37(b)(2)(C). *See In re Sept. 11th Liab. Ins.*

Coverage Cases, 243 F.R.D. at 130 (finding “negligence or worse” and imposing monetary sanctions where counsel obtained a relevant document in March 2003, but “left it buried in a box for nearly two years,” during which time they “fail[ed] to recognize” its importance even “when alerted to its possible existence by opposing counsel”). The reimbursable expenses include Infomir’s attorney’s fees, expert fees, and other costs reasonably incurred in obtaining and enforcing the 4/25/18 Order and the 7/3/18 Order (including the Vidulich deposition), as well as the expenses reasonably incurred in litigating the instant sanctions motion.³⁶

“The Court has wide discretion to apportion Rule 37 monetary sanctions between a party and its counsel.” *Joint Stock Co. Channel One*, 2017 WL 3671036, at *20 (collecting cases). In this case, the sanctionable conduct was committed by counsel. Effective deterrence therefor demands that the monetary sanction also run against counsel. *See, e.g., Yeboah*, 2000 WL 1576886, at *4 (awarding sanctions against “counsel personally” where “his own conduct, including

³⁶ Although Infomir could have pressed plaintiffs to produce the ESI underlying the Wireshark Investigation at any time after the Vidulich Affidavit was filed, it did not do so until April 2018, when it subpoenaed Vidulich and sought an order compelling plaintiffs to produce “the electronically stored data from the ‘network protocol analyzer’ referenced in Mr. Vidulich’s affidavits.” Joint Ltr. dated Apr. 16, 2018, at 4. Prior to that, although Infomir sought (and obtained) an order directing plaintiffs to supplement their response to document request No. 56, it voluntarily limited that order to tests that “plaintiffs, not their attorneys, have done,” 2/9/18 Conf. Tr. at 121:15-19, thereby excluding the Wireshark ESI. Plaintiffs are not required to reimburse Infomir for the cost of those (or earlier) discovery proceedings. Moreover, while Infomir argues with some force that plaintiffs’ failure to produce the Channel One PCAP “permeated all aspects of this case,” Infomir Moving Mem. at 21, and undermined its ability to respond effectively to plaintiffs’ motions to amend and for summary judgment, that species of prejudice bears no particular relationship to the expenses that Infomir incurred while so responding. Thus, plaintiffs are not required to reimburse Infomir for those expenses. *See also Yeboah v. United States*, 2000 WL 1576886, at *5 (S.D.N.Y. Oct. 20, 2000) (“Since the specific purpose of Rule 37 is to provide an array of sanctions for a party’s discovery failures, the only time for which a party can legitimately be compensated as a sanction is time spent during the discovery phase of the case.”).

misrepresentations and repeated dishonored commitments, wasted the time and resources of [defendants] and the Court”).

Neither plaintiffs nor Infomir has briefed the question of whether or to what degree plaintiffs themselves should be liable for Infomir’s expenses. It is possible that Dunnington was silent on this issue to protect its clients, or to avoid “compromis[ing] attorney-client confidentiality.” *Merck Eprova AG v. Gnosis S.P.A.*, 2010 WL 1631519, at *6 (S.D.N.Y. Apr. 20, 2010). The question is further complicated by the involvement of a non-party client, Kartina, which helped Dunnington set up the Wireshark Investigation but failed to provide even the minimal follow-up that would have alerted counsel to the central inaccuracy in the Vidulich Affidavit. *See* Hr’g Tr. at 114-15 (Dietrich) (“If I would see the affidavit, I will [sic] correct him about how the set top box communicate[s] with the server and where the video is coming from.”).

Under these circumstances, the Court elects “not to apportion liability” among plaintiffs, their counsel, and Kartina. *Merck Eprova*, 2010 WL 1631519, at *6. Even if the Broadcasters were uninvolved in the discovery misconduct committed on their behalf, it would ill-serve both the specific and the general deterrence goals of Rule 37 to allow them to escape sanctions by blaming “the incompetence of their trial counsel.” *Am. Cash Card Corp.*, 2000 WL 357670, at *5. As the Second Circuit explained in *Cine Forty-Second St. Theatre Corp.*, “A litigant chooses counsel at his peril.” 602 F.2d at 1064, 1065, 1068 (affirming a severe preclusion order, “tantamount to a dismissal of [plaintiff’s] damage claim,” where plaintiff failed to comply with a discovery order “due to a total dereliction of professional responsibility, amounting to gross negligence,” by its counsel). *See also New York State NOW*, 1997 WL 671610, at *5 (“[T]he acts and omissions of counsel are generally attributed to the client.”).

The monetary sanction will therefore run jointly and severally, without apportionment, against plaintiffs and their counsel of record, permitting them to settle the issue among themselves without further public motion practice. *See Merck Eprova*, 2010 WL 1631519, at *6 (reasoning that the disobedient party and its counsel were “best suited” to work out apportionment without judicial involvement).³⁷

3. Preclusion

Preclusion orders are often described as “severe,” particularly where the order sought would effectively terminate the litigation or eviscerate the disobedient party’s damages case. *See, e.g., Scantibodies Lab., Inc. v. Church & Dwight Co.*, 2016 WL 11271874, at *33 (S.D.N.Y. Nov. 4, 2016) (rejecting request that plaintiff be precluded “from offering any evidence of damages” as a sanction for the late disclosure of damages-related discovery, and instead recommending that discovery be reopened at plaintiff’s expense), *report and recommendation adopted*, 2017 WL 605303 (S.D.N.Y. Feb. 15, 2017).

The severity of the sanction, however, depends “on the nature of the proposed preclusion.” *Fitzpatrick*, 2013 WL 9948284, at *9. Thus, in *Fitzpatrick*, where defendant AIG negligently failed to retain data relevant to plaintiff’s damages calculation, the court rebuffed plaintiff’s effort to “preclude defendants from challenging in any way” the estimates of their own damages expert, calling that request “plainly overbroad.” *Id.* at 12. Instead, the court fashioned a “more limited remedy,” which precluded defendants from attacking plaintiff’s estimates only where those estimates were necessarily based on “data surrogates,” in the absence of the original data that AIG

³⁷ Should Dunnington and its clients be “unable to agree on apportionment of these sanctions, they may ask the Court to intercede.” *Merck Eprova*, 2010 WL 1631519, at *6.

failed to preserve. *Id.*; see also *Star Direct Telecom, Inc. v. Glob. Crossing Bandwidth, Inc.*, 2010 WL 3420741, at *6 (W.D.N.Y. July 23, 2010) (recommending a “limited preclusion order” preventing plaintiffs from offering evidence of damages resulting from a specific business arrangement, where defendant had to file three motions, including one for sanctions, before plaintiff produced the relevant documents), *report and recommendation adopted*, 2010 WL 3420730 (W.D.N.Y. Aug. 23, 2010); *Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, 2006 WL 3476735, at *8, *11 (S.D.N.Y. Nov. 30, 2006) (rejecting request for “broad preclusion of any evidence relating to public confusion, comparative product quality and dilution” as a sanction for plaintiff’s late and incomplete production of customer communications bearing on these issues, but issuing a “more limited” order “deeming as true” defendant’s contentions that none of the customer communications evidenced confusion, quality complaints, or dilution).

In this case, the remedy that Infomir seeks is “[a] limited preclusion sanction, applying only to plaintiffs’ reliance upon the May 2016 investigations.” Infomir Moving Mem. at 21. The order sought would not prevent plaintiffs from arguing or presenting evidence to demonstrate that Infomir engaged in unlawful streaming of plaintiffs’ programming; it would merely prevent them from relying on the Vidulich Affidavit, or the underlying Wireshark Investigation, for that purpose. According to plaintiffs themselves, this will be no great hardship, because they have adduced “overwhelming” evidence that Infomir is responsible for “a massive IPTV streaming operation.” Dietrich Decl. ¶ 71. See also Blaustein Decl. ¶ 50 (“Infomir’s sanctions allegations were a smokescreen designed to detract from the volumes of evidence against it”); 10/5/18 Tr. at 61:15-62-2 (attorney Dowd, arguing that plaintiffs “have much more” than the Vidulich Affidavit to show that Infomir is a “streaming defendant”); Joint Ltr. dated April 16, 2018, at 5 (plaintiffs,

resisting discovery regarding the Wireshark Investigation as “needlessly cumulative and costly” because plaintiffs could demonstrate Infomir’s piracy at any time using an iPad).

When asked to issue a preclusion sanction, the district court should consider (in addition to the factors listed above) “the prejudice that would be occasioned to the discovered party’s case by the proposed preclusion.” *Louis Vuitton Malletier*, 2006 WL 3476735, at *8. Here, it seems inconceivable that plaintiffs would be prejudiced by the exclusion of the Vidulich Affidavit (which they concede to be inaccurate in several key respects) or the Channel One Screenshots (which they concede to be non-probative of their claims). Moreover, although they now characterize the Channel One PCAP as “one of the best pieces of evidence in [their] case,” Hr’g Tr. at 6, plaintiffs have made no serious effort to demonstrate that its exclusion from evidence would prejudice them – and no effort at all to show prejudice disproportionate to the gravity of their misconduct.

I therefore conclude that the sanction proposed by Infomir falls at the milder end of the Rule 37(b) spectrum. Moreover, since the key evidence to be excluded is the same PCAP file that plaintiffs failed to recognize as probative in 2017, mislaid – and falsely claimed to be nonexistent – in 2018, and ultimately produced only after violating a series of court orders and facing spoliation sanctions, I also conclude that an order precluding plaintiffs from introducing or relying on that file is well-tailored to ensure that they “will not benefit from [their] own failure to comply” with this Court’s orders. *S. New Eng. Tel. Co.*, 624 F.3d at 149.

A review of the four *Agiwal* factors confirms these conclusions.

a. Willfulness and Reasons for Noncompliance

“Noncompliance with discovery orders is considered willful when the court’s orders have been clear, when the party has understood them, and when the party’s noncompliance is not due

to factors beyond the party's control.” *Thompson v. Jam. Hosp. Med. Ctr.*, 2015 WL 7430806, at *3 (S.D.N.Y. Nov. 20, 2015) (internal citation omitted); *accord Infinity Headwear & Apparel v. Jay Franco & Sons*, 2017 WL 4402541, at *5 (S.D.N.Y. Oct. 2, 2017). That standard is easily met here. The 4/25/18 Order and the 7/3/18 Order were clear. Attorney Blaustein's representations that Dunnington would extract the Wireshark data from the Firm Laptop, together with Vidulich's attempt to do just that, show that plaintiffs' counsel understood both orders. Moreover, plaintiffs' noncompliance was due entirely to factors within their own control. Indeed, viewing the evidence in the light *most* favorable to plaintiffs, the primary reason for their persistent failure to turn over the Channel One PCAP was a remarkable series of unforced errors by a poorly trained and technically incompetent investigator knowingly chosen – and inadequately supervised – by attorneys who sought to use his lack of expertise as a shield while blithely assuring the Court that no such file existed, and actively resisting Infomir's repeated efforts to persuade them otherwise, until threatened with spoliation sanctions, at which point they miraculously located the missing ESI on their investigator's desktop computer, precisely where he put it.

Plaintiffs' conduct was therefore not merely willful but, as Judge Preska put it in *Metro. Opera Ass'n*, “aggressively willful.” 212 F.R.D. at 222 (emphasizing counsel's “repeated representations of full compliance” made in the face of the opposing party's “continuing high-decibel allegations of failure to make adequate inquiry and repeated demonstrations of incomplete compliance and non-compliance with discovery requests”).

b. Efficacy of Lesser Sanctions

Infomir is correct that a monetary award alone cannot adequately serve the purposes of Rule 37 sanctions. Plaintiffs have litigated this case aggressively for more than three and a half

years, engaging in broad-ranging party and non-party discovery on two continents and peppering defendants with motions, many of them relying, directly or indirectly, on the Vidulich Affidavit.³⁸ At no time during this period have plaintiffs given any indication that they are constrained by budgetary limitations.³⁹ Moreover, as Infomir notes, plaintiffs' financing arrangement with Kartina may render them "immune," in whole or in part, "from the normal financial incentives governing good faith litigation." Infomir Moving Mem. at 22. A monetary sanction alone is therefore unlikely to have an adequate deterrent effect.

Nor will a monetary sanction alone ameliorate the prejudice that Infomir has suffered as a result of plaintiffs' discovery misconduct. The fact that the Channel One PCAP was ultimately "produced in advance of expert discovery," Pl. Opp. Mem. at 4, does not make its lengthy concealment "harmless." *Id.* Had it been timely produced as part of plaintiffs' automatic disclosures, or in response to Infomir's initial set of document requests, Infomir could have used it to challenge the allegations in plaintiffs' FAC, or in opposition to plaintiffs' first summary

³⁸ On May 24, 2019, while the instant motion was pending, plaintiffs moved for leave to file a Second Amended Complaint (SAC) that would, among other things, add a new defendant, "V-Net DBA Infomir USA," as well as new allegations concerning Infomir's conduct since the FAC was filed. Like the FAC, the proposed SAC alleges that "the Infomir Defendants both operate a pirate streaming service *and* manufacture and sell equipment and software designed to assist and profit from other pirates." Prop. SAC (Dkt. No. 751) ¶ 1 (emphasis in the original). Similarly, like the FAC, the proposed SAC attaches and relies upon the Vidulich Affidavit to support its allegations concerning Infomir's "pirate streaming service." *Id.* ¶ 249 & Ex. 27.

³⁹ On October 19, 2017, plaintiffs moved pursuant to Local Civil Rule 54.2 for an order requiring Infomir and another defendant, Goodzone, to post bonds in the amount of \$400,000 apiece as security for plaintiffs' costs. Goodzone cross-moved, pursuant to the same rule, to compel plaintiffs to post a bond. At that time, plaintiffs estimated that they had incurred over \$405,000 in legal fees and costs in connection with "motion practice with Infomir and Goodzone," and "anticipated additional legal fees and costs of between \$401,377.60 and \$601,033.60 to conduct discovery of Infomir and Goodzone." Pl. Mem. dated Oct. 19, 2017 (Dkt. No. 386), at 11. Both bond motions were denied. (Dkt. Nos. 616, 668.)

judgment motion (which was fully briefed before plaintiffs withdrew it), or – more generally – to better formulate and execute its overall litigation strategy, including the depositions of plaintiffs’ Rule 30(b)(6) witnesses (each of whom, as noted above, swore that the facts stated in the Vidulich Affidavit were true). Thus, “plaintiff[s]’ hopelessly belated compliance should not be accorded great weight.” *Cine Forty-Second St. Theatre Corp.*, 602 F.2d at 1068.

As an alternative to a preclusion order, plaintiffs suggest “another deposition” of Vidulich. Pl. Opp. Mem. at 3, 21-22. Had plaintiffs’ misconduct been confined to the first Vidulich deposition, a second deposition (at plaintiffs’ expense) might be an appropriate remedy. In this case, however, the prejudice to Infomir flows primarily from plaintiffs’ persistent failure to produce the ESI underlying the Wireshark investigation. Asking Vidulich more questions at this late date cannot cure that prejudice. A limited preclusion order, however, can even the playing field by prevent plaintiffs from taking unfair advantage of evidence that it withheld from its adversary during fact discovery. *See also* Fed. R. Civ. P. 37(c)(1) (prescribing preclusion as the presumptive remedy for a party’s failure to provide information or identify a witness as required by Rule 26(a) or (e)).

c. Duration of Period of Noncompliance

Courts “have found noncompliance for a period of several months sufficient to warrant dismissal or default.” *Urbont v. Sony Music Entm’t*, 2014 WL 6433347, at *3 (S.D.N.Y. Nov. 6, 2014) (granting default sanctions). *See, e.g., Agiwal*, 555 F.3d at 303 (affirming order dismissing case where plaintiff defied magistrate judge’s discovery orders “over a span of approximately six months”). Lesser sanctions are frequently imposed after a “relatively short” period of noncompliance, particularly where, as here, the underlying documents were “long overdue” by the

time the discovery order was issued. *3801 Beach Channel, Inc. v. Shvartzman*, 2007 WL 879668, at *4, *6 (E.D.N.Y. Mar. 21, 2007) (issuing monetary sanctions on March 21 for defendants' failure to produce documents due, pursuant to the court's orders, on January 8); *New York State NOW*, 1997 WL 671610, at *4 (issuing conditional order of preclusion where defendants failed to fully comply with production order for five months).

In this case, plaintiffs were out of compliance with their discovery obligations for more than two years. Even after the Court ordered them to produce the ESI underlying the Wireshark Investigation on April 25, 2018, it took them almost six months to disclose the Channel One PCAP (during which period I issued, and they violated, the 7/3/18 Order as well). In the meantime, Infomir was required to take Vidulich's deposition without the ESI from which he could have been effectively cross-examined,⁴⁰ and was further required to perform its own forensic examination of the Firm Laptop (work that plaintiffs should have done themselves) in order to assist plaintiffs in finding and producing the electronic file that they mislaid.

d. *Warning*

"Parties and counsel have no absolute entitlement to be 'warned' that they disobey court orders at their peril." *Daval Steel Prods.*, 951 F.2d at 1366. "Discovery orders are meant to be followed." *Bambu Sales, Inc. v. Ozak Trading Inc.*, 58 F.3d 849, 853 (2d Cir. 1995), *abrogated on other grounds by 4 Pillar Dynasty LLC v. New York & Co., Inc.*, 933 F.3d 202 (2d Cir. 2019). "A

⁴⁰ Plaintiffs produced the Channel One XPS prior to the Vidulich deposition. However, when Infomir's counsel asked Vidulich about the "source" of that XPS file, attorney Dowd instructed the witness not to answer on the ground that the question went "way outside the scope of his declarations." Vidulich Dep. Tr. at 99:5-16. Thereafter, plaintiffs falsely claimed that the Channel One XPS was irrelevant to the Vidulich Affidavit because it was the product of an unrelated (and fictitious) "preliminary" Wireshark investigation. Pl. Ltr. dated Sept. 21, 2018, at 3; 6/21/18 Vidulich Aff. ¶¶ 14-15.

party who flouts such orders does so at his peril.” *Update Art*, 843 F.2d at 73. *See also Grammar*, 2016 WL 525478, at *4 (S.D.N.Y. Feb. 8, 2016) (quoting *Gurvey v. Cowan, Liebowitz & Lathman, P.C.*, 2014 WL 715612, at *6 (S.D.N.Y. Feb. 25, 2014)) (attorneys are “chargeable with knowing the consequences of violating a court order”). In this case, moreover, plaintiffs and their counsel are no strangers to discovery sanctions, having frequently moved for severe penalties against various defendants, including Infomir.⁴¹ I therefore conclude that plaintiffs were adequately informed that violation of the 4/25/18 Order and the 7/3/18 Order could lead to sanctions.

V. CONCLUSION

For the reasons stated above, Infomir’s motion is GRANTED.

It is hereby ORDERED that plaintiffs are precluded from introducing or relying on the June 24, 2016 Vidulich Affidavit, any other report of, testimony about, or opinions based on the

⁴¹ On October 17, 2016, plaintiffs moved against defendant Panorama Alliance LLP (Panorama) and its counsel, seeking Rule 37(b) sanctions up to and including the entry of a default judgment, together with a fee award. (Dkt. No. 127.) I granted the motion, directed that certain facts be taken as established, and awarded a monetary sanction against Panorama and its lawyer, jointly and severally. *Joint Stock Co. Channel One*, 2017 WL 3671036, at *27. The award was later fixed at \$61,475.97. (Dkt. No. 747.) On October 10, 2017, invoking 18 U.S.C. § 401 and the Court’s inherent authority, plaintiffs moved for adverse inference sanctions, civil and criminal contempt orders, and an “award of statutory damages of at least \$20,000,000” against Panorama and defendant Asaf Yevdayev – both of whom had by then defaulted – for violating this Court’s post-default discovery orders. (Dkt. No. 372.) I analyzed the motion pursuant to Rule 37(b) and granted it to the extent of drawing an adverse inference, taking certain facts as established, and awarding fees. *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2018 WL 4760345, at *11-14 (S.D.N.Y. Sept. 28, 2018). On September 14, 2018 – the same day that Infomir first sought leave to file a spoliation motion against plaintiffs – plaintiffs filed a letter-motion seeking sanctions pursuant to Rule 37(b) against Infomir for failing to produce various documents. (Dkt. No. 662.) Plaintiffs requested, among other things, that the Court find certain facts to be true, authorize them to conduct additional discovery against Infomir (after the fact discovery close), and award a monetary sanction. *Id.* I granted the motion in part, directing Infomir to produce certain email attachments. (Dkt. No. 679.) However, “[g]iven the extent to which plaintiffs’ application overreached,” I found that “an award of expenses would be unjust.” *Id.*

May 2016 Wireshark Investigation, and any data or information captured during that Wireshark Investigation (including but not limited to the Channel One PCAP, the Channel One XPS, the Channel One PDF, and the Channel One Screenshots), except in response to any use of the same evidence by Infomir.

It is further ORDERED that plaintiffs and their counsel shall reimburse Infomir for its attorney's fees, expert fees, and other expenses reasonably incurred in obtaining and enforcing the 4/25/18 Order and the 7/3/18 Order (including the Vidulich deposition), as well as its expenses incurred in litigating the instant sanctions motion. Infomir shall file one or more declarations setting forth those expenses no later than **October 11, 2019**, and shall authenticate and attach the relevant time and expense records, including attorney time records and invoices for out of pocket expenses. Plaintiffs may file responding papers, limited to the amount of fees and costs to be awarded, no later than **October 25, 2019**. There shall be no reply.

It is further ORDERED that the parties shall meet and confer concerning the remainder of the pretrial schedule in this action, including expert discovery, and shall submit a proposed scheduling order no later than **October 11, 2019**. The proposed order shall also address the status of plaintiffs' motion for leave to file a Third Amended Complaint (Dkt. No. 748) in light of the fact that the proposed pleading attaches and relies upon the Vidulich Affidavit. If the parties disagree, they shall submit a joint letter attaching the competing versions of the proposed order and succinctly describing the areas of disagreement, without argument.

The Clerk of Court is respectfully directed to close the motion at Dkt. No. 692.

Dated: New York, New York
September 26, 2019

SO ORDERED.

A handwritten signature in blue ink, appearing to read 'Barbara Moses', is written over a horizontal line.

BARBARA MOSES
United States Magistrate Judge

Channel One Capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.12.136

No.	Time	Source	Destination	Protocol	Length	Info
54	15.509021	192.168.12.136	37.48.77.49	HTTP	665	POST /load.php HTTP/1.1 (application/x-www-form-urlencoded)
55	15.596540	37.48.77.49	192.168.12.136	HTTP	289	HTTP/1.1 200 OK (text/html)
56	15.596827	192.168.12.136	37.48.77.49	TCP	66	50715 → 80 [ACK] Seq=2321 Ack=4104 Win=2312 Len=0 TSval=1602455 TSecr=135510591
72	22.970968	192.168.12.136	66.234.224.2	DNS	90	Standard query 0x1c60 A freetvstat.iptv.infomir.com.ua
73	22.980869	66.234.224.2	192.168.12.136	DNS	90	Standard query response 0x1c60 Refused A freetvstat.iptv.infomir.com.ua
74	22.981285	192.168.12.136	8.8.8.8	DNS	90	Standard query 0x1c60 A freetvstat.iptv.infomir.com.ua
76	23.035708	8.8.8.8	192.168.12.136	DNS	106	Standard query response 0x1c60 A freetvstat.iptv.infomir.com.ua A 79.142.197.4
77	23.037415	192.168.12.136	79.142.197.4	TCP	74	44657 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=1609895 TSecr=0 WS=16
78	23.160212	79.142.197.4	192.168.12.136	TCP	74	80 → 44657 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1428 SACK_PERM=1 TSval=657155035 TSecr=1609895 WS=128
79	23.160468	192.168.12.136	79.142.197.4	TCP	66	44657 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=1610018 TSecr=657155035
80	23.163171	192.168.12.136	79.142.197.4	HTTP	591	PUT /00:1a:79:09:7a:de HTTP/1.1 (application/x-www-form-urlencoded)
81	23.285172	79.142.197.4	192.168.12.136	TCP	66	80 → 44657 [ACK] Seq=1 Ack=526 Win=15616 Len=0 TSval=657155066 TSecr=1610019

Frame 12: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface 0

Ethernet II, Src: Telecommu_09:7a:de (00:1a:79:09:7a:de), Dst: Dell_67:34:b6 (5c:26:0a:67:34:b6)

Internet Protocol Version 4, Src: 192.168.12.136, Dst: 37.48.77.49

Transmission Control Protocol, Src Port: 50715 (50715), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 305

Hypertext Transfer Protocol

0000 5c 26 0a 67 34 b6 00 1a 79 09 7a de 08 00 45 00 \&.g4... y.z...E.
0010 01 65 a9 65 40 00 40 06 50 9c c0 a8 0c 88 25 30 .e.e@. P.....%
0020 4d 31 c6 1b 00 50 05 c0 74 3b 76 d1 4c fc 80 18 M1...P.. t;v.L...
0030 04 e2 6f 73 00 00 01 01 08 0a 00 18 52 64 08 13 ..os.... ..Rd..
0040 98 9e 47 45 54 20 2f 70 75 62 6c 69 63 5f 68 74 ..GET /p ublic_ht
0050 6d 6c 2f 3f 6c 61 6e 67 75 61 67 65 3d 65 6e 26 ml/?lang uage=en&
0060 6f 6e 6c 79 3d 6f 6e 6c 69 6e 65 5f 63 69 6e 65 only-onl ine_cine
0070 6d 61 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 ma HTTP/ 1.1..Use
0080 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
0090 2f 35 2e 30 20 28 51 74 45 6d 62 65 64 64 65 64 /5.0 (Qt Embedded
00a0 3b 20 55 3b 20 4c 69 6e 75 78 3b 20 43 29 20 41 ; U; Lin ux; C) A
00b0 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 33 2e 33 ppleWebK it/533.3
00c0 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 (KHTML, like Ge
00d0 63 6b 6f 29 20 4d 41 47 32 30 30 20 73 74 62 61 cko) MAG 200 stba
00e0 70 70 20 76 65 72 3a 20 33 20 72 65 76 3a 20 33 pp ver: 3 rev: 3
00f0 38 37 20 4d 6f 62 69 6c 65 20 53 61 66 61 72 69 87 Mobil e Safari
0100 2f 35 33 33 2e 33 0d 0a 43 6f 6e 6e 65 63 74 69 /533.3.. Connecti
0110 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a on: Keep -Alive..

Channel One Capture

Packets: 2087 · Displayed: 1937 (92.8%) · Load time: 0:0.69

Profile: Default

11:11 AM
5/21/2016

Appendix